phdprojectsorg@gmail.com
+91 98946 59122

Secure Opportunistic Network

Abstract

Researchers have started investigating the development of the Opportunistic Network, which seeks to create a platform for the development of a new form of wireless communication. Unlike traditional networks, which require a continuous connection between two points for packets to be transmitted, OppNets enable mobile nodes to receive packets, carry, and forward them to another mobile node. Therefore, OppNets are best used in offering communications in disaster recovery operations, military operations, remote areas where traditional cellular communications are non-existent, connected car networks such as taxi fleets, smart cities, smart towns, wearable medical monitors, IoT, etc., and even locations characterized as urban. However, the major issues of OppNet routing are inherent to using a store-carry-forward kind of communication model, due to the following reasons: node movement pattern is usually highly unpredictable, links are disrupted frequently, lack of any form of centralized control, and resource constraints such as bandwidth and energy are very limiting factors which, in conjunction, make routing in OppNets complex, slower, and non-scalable when benchmarked against traditional cellular networks. Limitations in existing Opportunistic Routing Protocols: Basically because of their inability to reach an optimal balance between two important factors crucial for routing protocols: reliable message delivery and efficient exploitation of the available resources. Initial opportunistic data routing methods, such as the Epidemic Routing of data means, have used floods of replication, orderly message floods. These approaches improved message delivery rates at the cost of added overhead from routes, buffering, energy consumption, and poor scalability, among others. The protocols that proposed Quota methods to address this problem, like Spray and Wait, work on providing limitations to message replication. However, most of these do not adapt or adjust themselves as the network and/or node circumstances change. The Prediction and Probability-Based protocols mostly count on historical information linked with the nodes when delivering a particular piece of information in order to determine the probability of consistent encounter with a particular node. The effectiveness of such a method could be

compromised in a dynamically changing heterogeneous network. There is additional complexity, communication, and computation associated with Community-Based, Trust-Based, and Reinforcement Learning-Based methods for delivering messages, which makes them impractical for large-scale implementations in Opportunistic Networks. The two most important factors in Opportunistic Networks include Privacy and Security. In an OppNet, as there is no central controller that can be relied upon, they function in a continuous manner, unlike traditional networks. Here, regular cryptographic means of secure transmission, as in the usage of certificates or pre-positioning of keys, cannot be followed in OppNets. The type of attacks faced by the OppNet includes dropping packets, selective forwarding, injecting false feedback, impersonating a node, or behaving selfishly. The use of security systems that are based on Trust and/or Reputation systems has been proposed to resist these attacks; however, these systems are plagued by certain drawbacks, including the fact that there are considerable delays in the evaluation of the level of trust. The use of artificial intelligence models, deep learning models, and blockchain technology is becoming more prominent in order to counteract the aforementioned drawbacks. However, these models are plagued by their own drawbacks. The existing models that describe the secure solutions for OppNets are mainly considering spatiotemporal features; however, these models are not considering or evaluating some critical contextual parameters that are equally important for the proper functioning in a security context, including: Stability of nodes; Residual energy; Buffer state; Co-operation behavior; and Mobility dynamics. Mobility Models complicate the efficient and secure design of OppNet Protocols. Current mobility models are based on random, socially aware, Campus-based, Markovian, Fuzzy and Bursty Contact Model's, with the majority of these models depending upon Historical Contact Data, i.e., Static or Historical Social Relationship Data, i.e., Static. It would also be apt to mention here that while mobility models provide improvement in comparison with ground reality, their working in rapidly changing environments and large heterogeneous scale networks is pretty inefficient compared to the current methodologies. Hence, this relies more on Cache Coordination Sharing and Historical Data Processing, thereby introducing extra Communication and Storage Overhead, reducing the Energy Efficiency and scale. Based on this, the dissertation aims to propose an innovative and groundbreaking approach that is integrated, lightweight, adaptable, and has the capability to ensure effective routing and security/privacy for opportunistic networks. The goal of this research is to formulate an approach that is scalable, minimizes routing costs, ensures reliable

routing, and has the capability to protect the network from selfish and malicious behavior, ensuring security and reliability for end-to-end data transfer and communication.

Particularly, it increases the efficiency of message routing by assessing the stability of each node using criteria such as patterns of mobility, duration of encounter, available buffer space, and accessible energy, in order to prevent more copies of messages being sent and ensure their delivery. In order to address issues related to cooperation and security in opportunistic networks, the dissertation will establish a Security- and Privacy-Oriented Opportunistic Networking Scheme (SPONS) that incorporates the opportunistic cooperativity and incentivized trust management between nodes within such networks, along with detection of selfish nodes. The proposed model, SPONS, makes use of the SORSI (Social-based Opportunistic Routing with Selfishness Detection and Incentive Mechanism) security framework. The SORSI security mechanism uses an encounter-based selfishness score for dynamic detection of uncooperative nodes and provision of incentives for cooperative nodes. Using the Selfish Node Identification component of the opportunistic network SPONS framework, we determine how much a certain opportunistic network node in an opportunistic network is involved in the network using the forwarding behavior of the opportunistic network nodes as a measure of how cooperative it is in the network. When an opportunistic network node acts as a dishonest or a selfish node, it is possible to detect these nodes. In contrast to conventional trust-based schemes that incorporate feedback from the participating nodes and provide it to another opportunistic network node after a delay in terms of time, the SPONS framework, on the other hand, aims to provide immediate feedback on the behavior of the opportunistic network node, let alone consider building a precise model that aims to measure the authenticity of the feedback received and consider applying the corresponding actions with regard to a specific opportunistic network node. Due to the provision of feedback and the direct measures taken to consider the evaluation of the opportunistic network's behavior, it is to be expected that the SPONS framework would be effective in preventing attacks such as the insertion of false feedback and the selective forwarding. The proposed framework will incorporate Hierarchical Identity-based encryption for end-to-end secure communication with little or no key management overhead. It allows a cryptographic key to be directly linked to that of the user or node. This negates the need for a centralized certificate authority, and also a complex key distribution structure. Encryption is based on the identity of the node, so in case this encryption traverses through many nodes, it will retain its confidentiality and integrity, and the identity of the sender. Also, HIBS deploys much simpler

and light-weight cryptographic scheme for encryption compared to traditional public-key infrastructures. Therefore, HIBS is ideal for resource-limited mobile device users and for opportunistic communications where many data packets can be transported at once. Using the ONE simulator, we evaluate the effectiveness of our proposed framework through extensive realistic mobility scenarios and various flows of traffic over various numbers of hops. Metrics include Delivery Ratio (DR), Average Latency (AL), Overhead Ratio (OHR), Buffer Utilization (BU), and Energy Consumption (EC). Comparison is made against all current state-of-the-art protocols in the areas of Routing Protocols (RPs) and Security Protocols (SPs). Simulation results have demonstrated that our proposed framework persistently outperforms existing protocols in terms of DR and OHR, while maintaining acceptable levels of latency. The results that can be expected from such an approach will include stability-aware routing and cooperative security mechanisms, with significant resilience to both selfish and malicious nodes at low computational and energy costs. This dissertation gives an overview of key areas of opportunity in pursuit of continued evolution of opportunistic networks. Within this dissertation, it has been possible to develop a comprehensive and adaptive framework which is effective in joint optimization of opportunistic network efficiency, security, and privacy. It is considered that such a solution is applicable and viable as an effective means of creating sufficiently dependable and secure networks. Strategies utilized in this research have been based on awareness, cooperation among devices in an OppNet, and encrypting such data at low cost and effort. Overall, the results from this research serve as the basis upon which future generations of Opportunistic Networks can be designed, allowing for experimentation with applications for opportunistic networking in realistic scenarios, cross-layer optimization, and creating next-generation mobility-aware security protocols. Opportunistic Networks can achieve connectivity among nodes that are not mutually connected through an unbroken end-to-end path by utilizing a Store Carry Forward Communication Model. Opportunistic Networks are currently being utilized for Disaster Recovery, Military Communication, Remote Connection, Vehicular Networks (cars), Smart Network Cities, and Internet of Things (IoT). The hurdles associated with mobile nodes and the uncertainties related to connectivity periods among nodes, and the significant limitations on energy availability, storage capability, and bandwidth for all Opportunistic Networks, are compounded by security and privacy problems, as any kind of standard certificate-based cryptographic algorithms are not applicable to a distributed system. This paper proposes an agile and flexible framework for creating opportunistic networks. The

integration will take into account routing that is dependent on network stability, as well as cooperation-oriented approaches to network security and identity-based encryption, which will yield adequate success in messaging with little network usage. The Scheme for Security- and Privacy-Centric Optimistic Proximate Networking (SPONS) will be utilized to establish an approach that is effective in the identification of nodes operating in an inefficient manner, including their collaboration and forwarding patterns and rewarding nodes that exhibit cooperation in the network. An innovative framework for secure end-to-end communication, including low-key management, termed Hierarchical Identity-Based Encryption (HIBE), has been designed. Using the ONE simulator, an increase in ratio and a reduction in network overhead have been achieved compared to the most recent approaches in opportunistic routing and security. Additionally, the framework that is being proposed in this particular piece of work is also suggesting that it is important for context-aware decision mechanisms utilized in opportunistic networks not only take into consideration routing stability, cooperation behavior, and security aspects - that is, it utilizes and makes use of these three aspects of knowledge individually rather than collaboratively as one united front. As opposed to what is traditionally believed and demonstrated with regard to these three aspects of knowledge being independent and unique concepts in and of themselves, it is being demonstrated in this piece of work that by tightly coupling these aspects of knowledge and ensuring that they stay at the forefront and at the heart of one singular concept known as an integrated whole network model, one is actually being provided with demarcation and clarity from a standpoint that is significantly better for utilization and understanding. The main benefit of this proposal is that it can function extremely well in a heterogeneous, and highly dynamic environment. As a result, there would be reduced replication of messages and yet a high probability of delivery. This addresses some of the issues of scalability that might be experienced as a result of having opportunistic networks. The fact that a cooperative model is being employed guarantees all the participants a reduced likelihood of engaging in selfish behaviour. In addition, there would be reduced harm from malicious behaviour without creating a burden to other participants. The incorporation of incentive-based collaborative approaches would be made into existing approaches of assessing a network's reliability. Therefore, through the aspect of cooperation, more participants would be available to take part in the forwarding of the messages. As a result, nodes that are cooperative would be rewarded within the network, and those that act selfishly would be eliminated from the network based on behaviour. These actions would create a perfect environment of trust

between the participants and to establish incentives to build relationships without requiring central authority to monitor and control activities in the network. Further, this model uses hierarchical identity-based cryptography that accommodates confidentiality, authenticity, and integrity services for information contained in message payloads from the time of storage until delivery using the store-carry-forward paradigm. When it comes to the use of encryption keys in place of identity to safely build up a communication channel from one of your nodes to another without having to repeatedly exchange keys in a central point of control, it creates the possibility for much more efficiency in terms of reducing the overall cost of cryptography. However, the proposed model can properly function in the context of mobile devices with less power and resource availability. The framework has been tested numerous times using different models in ways that accurately describe normal human movement patterns and can function well for all levels of traffic in a network, regardless of whether it functions well or not). The results of the simulations revealed that there is an increasing relationship between the number of messages sent and delivered and an acceptable level of both the time it took for these messages to be sent and received and the energy used in the devices involved in either sending and/or receiving these messages. As evidenced by the results of the simulations included in this dissertation, it is possible for an overall system that is designed for validation of implementation of the model recommended in this dissertation and is characterized by key elements such as sporadic and/or restricted resources to be created. This dissertation is intended for use as a way of creating a system that is used for validation of malicious acts where it is possible for packets that are being sent and/or received through such networks as opportunistic networks to be routed, with consideration of user security as well as the cooperative and collaborative nature that is inherent in devices used in such networks. It is also evident from the results of this dissertation that it is possible to construct various types of routing solutions, including security routing solutions, that can be used in ascertaining the optimal manner such research it will also offer opportunities for further research to be conducted, illustrate how the research is applicable to the real world, illustrate how to utilize various viable information sources on numerous levels of information, illustrate how to utilize emerging technologies like the Internet of Things and 6th Generation Technology to accomplish the required goals, and illustrate how to use various security protocol systems to ensure the security of the packet delivery from users to their destinations. As mentioned earlier, the results of this dissertation suggest ways to build

highly reliable, secure, and function communications to help deal with the changing decentralised network world.

Table of Contents

List of Figures

List of Tables

Chapter 1

Opportunistic Networks represent a new communication paradigm that enables data exchange in dynamic, infrastructure-less environments using a store–carry–forward mechanism. While they offer significant benefits for applications such as disaster recovery, defense, smart cities, and IoT, they face challenges including intermittent connectivity, limited resources, scalability, and security. This chapter introduces the fundamentals and motivation of Opportunistic Networks, defines the research problem, and presents an integrated adaptive routing and cooperative security framework to improve network performance, security, and resilience.

Section 1.1 discusses major OppNet challenges such as intermittent connectivity, routing overhead, scalability and security. Section 1.2 provides the motivation for this work, and discusses the need for efficient, secure, adaptive communications in dynamic environments. Section 1.3 provides the problem statement and introduces the solution proposed in this research - an integrated routing and security framework incorporating the STCESW-DSA routing protocol and the SPONS security protocol. Section 1.4 provides the research objectives, which include improvements in routing performance, enhancement of security, and support for scalability. Section 1.5 describes the scope of this study, including its focus on routing and security layers, as well as limitations of the work. Finally, Section 1.6 provides the organization of the thesis and Section 1.7 provides a summary of major points from this chapter.

Introduction

1. Mobile Ad-hoc Network (MANET)

Wireless multi-hop networks, especially ad hoc networks, have been focused on due to their potential as a robust architecture, especially due to their ability to support the autonomous, self-organized, and distributed management of network communications for applications such as the Internet of Things (IoT), where infrastructure might not be present due to some reason (natural disaster for example). The self-organized characteristics of ad hoc networks can facilitate the provision of communication opportunities, which may only be achieved by using terminals or devices that comprise an ad hoc network. There are several benefits associated with deploying ad hoc networks, including low cost of deployment, adaptability to the environment, quick-to-deploy, and others. Opportunistic Computing is a form of pervasive computing that uses the properties of a Mobile Ad hoc Network, such as randomness and uncertainty, to create an opportunity for devices to connect opportunistically [11,94].

2. Delay Tolerant Network (DTN)

These systems use the store-carry-forward method of communication to communicate between users. Mobile nodes save messages until an appropriate opportunity to communicate with another user comes up, and then forwards these messages to that user when an opportunity occurs. In some ways, opportunistic networking is similar to the store-carry-forward topology used by mobile ad hoc networks, in that opportunistic networks provide a flexible way to store and transmit data [12]. A variety of challenged networks (OppNet) exists that is defined as an environment in which an end-to-path between nodes cannot be established and guaranteed for all nodes due to the fact that they have temporarily connected and disconnected from each other due to the transitory nature of node mobility [170,172,183]. Because of this diversity of connectivity and node movement within an OppNet, routing of information between nodes will be an ongoing challenge.

3. Opportunistic Network (OppNet)

Opportunistic Networks (OppNets) are a unique type of wireless network developed for use in extremely unstable, no-infrastructure environments, where consistent connections between devices (end-to-end) cannot be assured. OppNets provide a way of enabling communications between users in the aftermath of natural disasters, as well as in rural areas/remote locations, military operations, vehicles, and the growth of the IoT in areas subject to constant change [1]. Unlike regular mobile ad hoc/infrastructure networks, OppNets are characterized by the unpredictability of the movement of nodes and nodes' inability to consistently stay connected (intermittent connectivity). Additionally, OppNetworks have a distributed control structure. Nodes have the ability to configure themselves into out-of-links depending on their proximity and movement patterns; therefore, routing becomes difficult for an OppNetwork as it develops. Over time, OppNetwork routing techniques have gone from very basic forms of flooding-type routing protocols to the more complex routing types such as Context-Aware Routing and Trust Routing; Reputation Routing and Community Routing; and Learning Routing [2,3]. Improved routing protocols are designed to enhance the quality of data delivery and to reduce the amount of overhead normally associated with routing. They are also designed to optimise usage of scarce resources (i.e., buffer space, energy, and bandwidth), which are limited at individual nodes [4]. In addition to improved efficiency and security with respect to routing, the unpredictable nature of mobility and disconnection still presents challenges to Routing. Protocols many challenges, such as increased latency, congestion in buffers, excessive replication of messages, and scalability issues. In addition, OppNets have no central authority they're vulnerable to many of the following types of attack due to the open wireless interface used for transmissions. Users may not cooperate with each other and will cause issues by dropping packets and by injecting false feedback (messages). Messages may also be selectively forwarded by malicious users. Traditional cryptography is typically not applicable for these types of networks because of the complicated key-management requirements and resource limitations of mobile nodes [5-10]. Research within the last few years has examined techniques such as Using Artificial Intelligence, the use of Deep Learning, the use of Trust and Reputation frameworks, and using Blockchain-assisted means to secure routing, detect attacks, and securely forward data. Mobility models were also proposed that better reflect actual node movements based upon modelling social behaviours, campus environments, and previous contacts. Unfortunately, many current solutions still have many negative issues they

suffer from, including high computational costs of running, and limited capabilities of adjusting to quick topological changes, lack of awareness of the user's current status and reduced effectiveness when presented with large volumes of users and very mobile environments [75, 77-79]. In recent years, there has been an increased focus on pervasive computing within the Wireless era. This has brought about the need for a new computing paradigm to allow for better organisation of our networking devices, which include all the modern mobile devices Smartphones and tablets that we use daily. Data routing and its transmission, as well as the security concerns regarding the data that has been transmitted, are two major challenges facing all forms of distributed databases today, but opportunistic routing will also continue to be a field of research for improving both energy efficiency and secure data transmission methods [29, 30,130,131,134]. The Opportunistic Networking paradigm may form the basis of IoT, enabling the opportunity to connect disparate WSNs through the use of mobile devices that are only occasionally present. Thus, providing new opportunities for communication within the WSN while providing alternative routing methods to reach the internet, it is based on sharing three main types of resources: power, energy, and memory among peers. Opportunistic Computing Opportunistic Networks use these three types of resources to exchange information with each other, thus creating a communication channel between devices without having an established end-to-end connection.

With new inventions being developed quickly, there is a great deal of interaction between various technologies in the wireless communications arena, and a fusion of cybersecurity technology and opportunistic networks (OppNets) will create a major shift in how wireless networks are formed and maintained [140,144-147]. This fusion of Cybersecurity and OppNets does not just represent the merging of two very different concepts and technologies, but rather the beginning of a completely new age in the wireless communications industry with many new innovations and greater opportunities for growth and development [71, 72]. Now, as we are entering the time when data transfer has become the most critical element for individuals and businesses, the need for a way to connect multiple users efficiently and dependably will move from a need based on cost-effectiveness to that of being able to do so sustainably and for the foreseeable future. However, the most significant difference is that opportunistic networks rely on creating communications between their members using the time, space, and opportunity for contact as a basis for contact, as opposed to the opportunistic networking aspect of the Store-Carry-Forward models that create point-to-point connections.

The rapid advancement of wireless technologies, coupled with the exponential growth in the amount of data being transmitted through mobile networks, will require a fundamental change in traditional routing algorithms. Current Opportunistic Routing techniques also have limitations in speed and Security during transmission [117,-120]. We will discuss and introduce a Community-Based method of deciding which information should be routed opportunistically based on trustworthy models. Using this algorithm, we can measure the trustworthiness of a node by considering its previous behavior when forwarding packets through the network. Using the model for calculating trustworthiness, we can determine the level of trust in the node and its position within the Trust Threshold and Trust Attenuation of the Security Community. When forwarding messages, the nodes that are located within the Security Community will be selected first as the next hop nodes, thereby providing assurance that the delivery of messages to the next hop will be secure and protected [13,14]. Opportunistic Networking also uses a new Technology to integrate Communication, Sensing, Storage, and Computation and allows for Greater Collaboration between Networks. The most important problem that arises in Wireless Sensor Networks (WSNs) is how to adequately cover your area of interest and convey the data back to the sink node without being reliant on only one node or one route. To do so, we will use a swarm-based dragonfly as our primary mechanism for routing data in this application. The dragonfly approach consists of two phases: an exploration phase, where global searching is performed, and an exploitation phase, where local searching is performed [192,194,200,201]. The routing algorithm is based on the inherent behaviors associated with swarming. OppIoT (opportunistic internet of things) networks pose a considerable challenge with regard to forwarding data between devices that do not cooperate with each other, which causes packet loss and additional delays in communication. As such, this article introduces a new protocol for OppIoT networks called the Context-Aware Trust and Reputation Routing protocol (CATR). By using a probabilistic density function that describes how nodes interact through the beta distribution, CATR calculates the trust and reputation values of other nodes in order to facilitate effective data dissemination by circumventing malicious nodes [65, 54, and 70,76]. Opportunistic Networks (OppNets) are a collection of connected smart devices and entities with the ability to move and establish a connection without any physical dependency on established infrastructure [67-69]. As a result, OPPNETS represent a highly valuable medium for the transmission of data during emergencies and disasters, including both manmade and natural occurrences. Nevertheless, the preservation of both message confidentiality and message integrity must be carefully maintained when transmitting physiological and critical condition data, due to the

legal constraints placed on how this type of data may be transmitted. To this end, we will describe an approach to classifying messages according to their relative level of importance through the use of several independently operated queues. On account of the decentralized nature of OppNets, we will also present an additional method for ensuring the security of the highest priority messages, by utilizing a blockchain-based structure [148-150,155,113]. This structure consists of three successive operations of functional blocks, which are implemented with the least amount of complexity, and as such, is ideal for operation with battery-powered wearable devices that are subject to limitations regarding energy consumption as well as processing units. Simulation results reveal that the average value of the variation in the size of the blocks of messages (after the addition of a node) is insignificant as the number of nodes in the network continues to increase [151,198]. This finding is critical to removing the bottlenecks that are created by the computational aspects of OppNets. Smart devices, capable of connecting to the Internet, are the new communication paradigm associated with the emerging Internet of Things (IoT). The Internet of Things (IoT) is an integrated network of devices and systems where smart devices, people, and wireless networks work together to deliver services [165-167]. The objective is to offer Internet access from any device capable of accessing the Internet or to establish a method of continuously monitoring and maintaining community-based network connections.

With the widespread adoption of the internet, we see that TCP/IP has proven to be a reliable means of communication, providing reliable communications for transferring data internationally. Many advantages exist with TCP/IP networks, including their ability to support high flexibility and adaptability. Nevertheless, there exist particular situations where TCP/IP may not work. For example, TCP/IP may not work for networks if the nodes are unable to establish a constant and continuous connection. Policies and requirements for forwarding information from the sender to a receiver are defined by the routing protocols used to route traffic [184,186, 187]. Depending upon the type of network being used and how the network operates, the goals of routing may be to send out "broadcast" messages to all nodes or to send data from node to "gateway nodes". Traffic control methodologies (including contextual information and node data) are commonly used to route traffic from one node to another. Recently, dozens of routing solutions have been created with specific regard for the social aspects of nodes [65, 98,102]. Algorithms have been developed that use information obtained from a node's historical usage patterns to determine which hop and which carriers to use. One of the contributing factors to the ongoing challenge of routing is

that the battery life of the mobile nodes is adversely affected by the multi-routing activities associated with OppNets (i.e., scan, transmit, receive, compute, etc.), which decreases the overall performance of the OppNet [122,123,125]. Opportunistic Networks are self-organizing, dynamic networks that facilitate the transmission of data by taking advantage of the available communication channels as nodes move about them. Because inter-node connections are made indirectly, opportunistic networks are highly vulnerable to malicious attacks and therefore pose significant challenges in securing their networks. This paper presents a Trust-Based Model for Secure Routing of Opportunistic Networks (TBMOR) because it uses both the Forwarding Positive Degree (FP) and Node Activity Degree (NA) when calculating the Trust Value of each node. The Trust Value of nodes is assessed using a combination of Direct Trust and Indirect Trust. Once the Trust Value for each node is computed, the next node to be routed through is optimized using both the Trust Value and the Pruning Strategy [158,164,169]. Additionally, this paper suggests that, by establishing Energy Thresholds dynamically throughout the network's lifecycle, your network can extend its lifecycle while reducing the amount of redundancy within the network by adjusting the number of Replicas that exist for any given piece of data using Trust Values [89]. Wireless communication began as a voice communication system using Radio Frequencies (RF) as the carrier wave for sending information. Over the last several decades, however, wireless communication has developed into an extremely complex and very dense interconnection of hundreds of thousands (if not millions) of interconnected devices. Digital modulations, frequency efficiency improvements, data transmission methods, and dramatic advances in physical layer technology are the technological foundation of this development and expansion [92,190,199]. Therefore, there is an urgent need for an integrated, lightweight, adaptable framework for combining efficiency related to route selection, security, and support for mobile users. In order to provide the most effective method for forwarding and relaying the messages, it will require robust, scalable, and resource-efficient qualities so that it can work in highly dynamic and opportunistic networking environments.

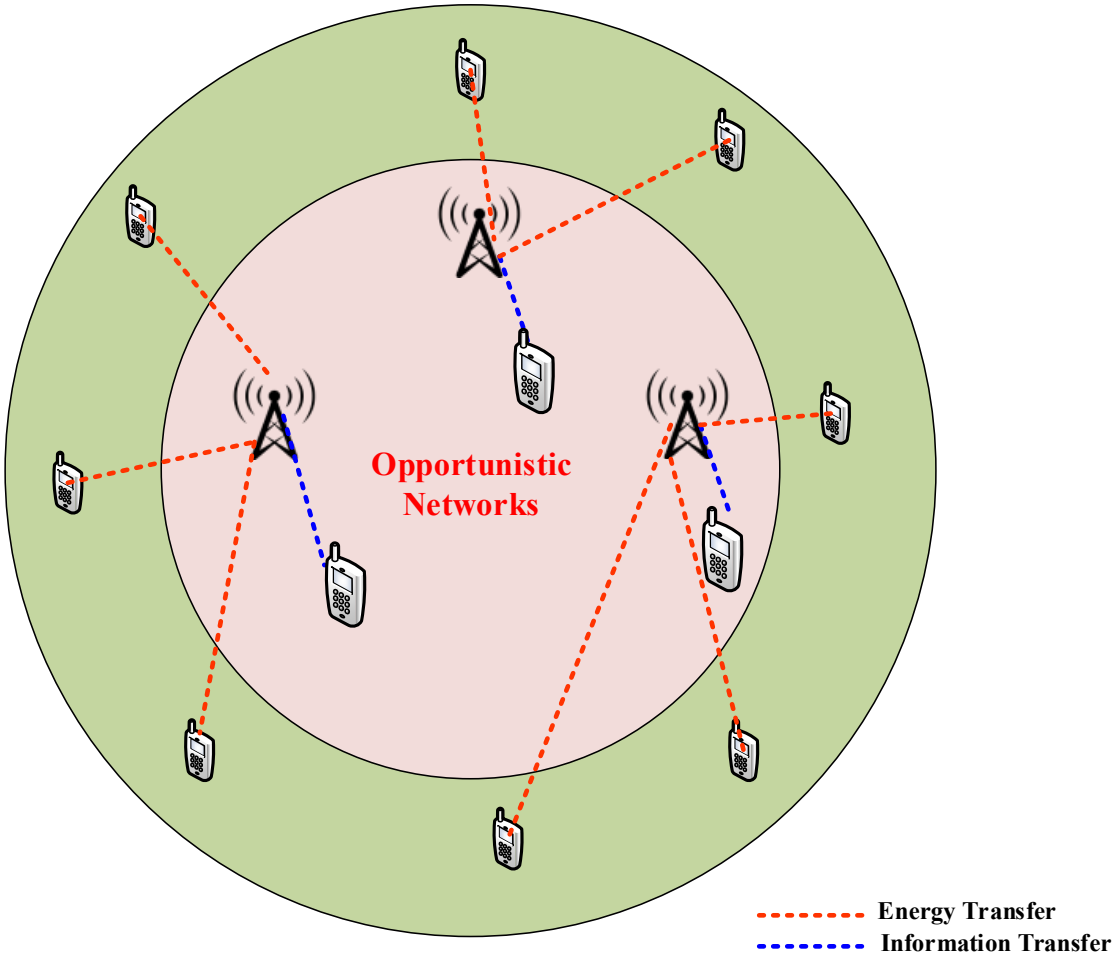

Fig1. 1 Opportunistic Networks

1.1 Challenges

The following points highlight some of the main obstacles faced by Opportunistic Networks (OPN) due to their distinctive way of working.

- **Links that Connect and Become Dynamic Networks:** The inconsistency of network routing caused by OppNets is due to the routing from a source node to a destination node not being a direct route but instead a series of links that may be broken due to the movement of mobile client nodes, along with the high frequency at which mobile client nodes change their routes from one to another as they continue to move.
- **Routing Resource Overhead:** Excessive reproductions of messages are produced through flooding replication routing methods; therefore, they generate a large number of messages with high overhead, possibility of message loss due to buffer overflow, excessive energy usage; and excess network congestion. An effective routing system will strike a balance between a high delivery probability and finite node resource constraints.
- **Scalability Problems:** Routing, clustering, and community-based approaches that currently exist have limited scalability because their computational complexities are too high and they have to pass through too many control messages back and forth between the participants, along with reliance on global or past network data.
- **Limitations of Cryptographic Methods and Complex Key Distribution:** Conventional methods of cryptographic security utilize a centralized authority and pre-distributed keys, which are not reasonable in the case of OppNets. Secure Communication must be established without the redundant burden of key management.
- **Routing and Security Models with Limited Contextual Awareness:** Routing and Security Models use only limited contextual information, such as: encounter probability, spatiotemporal data and not taking into consideration many other significant aspects such as: node behaviour, residual energy, buffer state and social characteristics.

- **Mobility Modeling Limitations:** The mobility modelling that exists currently is based upon either a) static social relationships, or b) historical contact data. Because of this, they do not provide the flexibility to accommodate the ongoing changes in user behaviour and the increase in scale of users. In addition, cache share and processing of historical data increases the communication and storage burden of these models.

1.2 Motivation

The rapid growth of mobile devices, Internet of things systems, and delay tolerant applications has significantly increased the importance of opportunistic Networks (OPPNets) for enabling communication in environments where continuous infrastructure based connectivity is unavailable. Scenarios such as disaster response, smart cities, military operations, rural communications and mobile edge environments require reliable, efficient, and secure data transmission despite frequent disconnections and highly dynamic network conditions. There have been many studies done regarding a variety of different types of networks such as routing, security, and mobility, within the field of OppNets, but nearly all current solutions have significant limitations.

Protocols based on flooding and probabilities improve the chance of successful delivery but create an increased amount of routing overhead, energy consumption, and buffer congestion. There are a variety of different types of routing solutions that use different methods for Computational complexity, limited scalability, and experience a large number of collecting information about forwarding decisions, including community-based, trust-based, and reinforcement learning-based; however, they generally have very high levels of interruptions. When there is a high level of node mobility that negatively affects their performance when used in an OppNet.

Security increases the difficulty of these challenges. Due to the lack of centralized control, as well as the intermittent connection and limited resources at the nodes, OppNets are particularly open to the effects of selfish and malicious behaviour. Crypto techniques based on traditional methods will not work since it is complicated to distribute keys. Solutions to this problem are limited because existing systems based on artificial intelligence and trust suffer from inaccurate trust evaluation, delayed feedback, vulnerabilities to complex attacks, and high computational and energy overhead. Additionally, many AI prediction models and deep learning models do not take full advantage of context when developing their security and prediction models. Consequently, these models do not achieve optimal detection performance.

In addition, mobility modeling is a major component of OppNet. Although existing models focus on social, contact-based, and campus-based, they are unable to adapt quickly to the rapidly changing environment or large-scale heterogeneous not having similar features. Their reliance on historical contact information and the use of cache sharing techniques also increases the communication overhead and restricts scalability.

The ongoing difficulties emphasize the necessity of designing a distributed, adaptive, light-weight framework that provides routing efficiency, mobility awareness, and secure communications for opportunistic networks. The objective of this dissertation is to create and evaluate a framework that has the ability to make stable-based decisions on routing and incorporate dynamic adaptation, cooperation-based security models, and implement identity-based cryptographic approaches. The goal of this research is to allow for scalable, efficient, and secure means of disseminating data when using opportunistic networking in real time by minimizing excess communications; improving delivery rate, identifying selfish participants; and providing secured communications with the least amount of overhead possible.

1.3 Problem Statement and Proposed Solution

- **Routing Inefficiency in Dynamic Opportunistic Networks:** Networks of Opportunities are operated by using a storage/forward communication method, and allow for decentralization of connections. The currently available routing protocols generate many copies of messages in order to allow for an increased probability that they will deliver; however, they produce a lot of overhead when routing, which leads to buffer overloads, battery drains, and fail to scale efficiently. Routing protocols that use prediction algorithms or machine learning encounter the same issues with loss of connection through routing, as well as loss of packets due to unpredictable movement from rapidly changing networks.
- **Limited Adaptability to High Mobility and Network Dynamics:** Most adaptive clustering algorithms, community-based routing protocols and energy-aware routing protocols assume stable links and extended periods of contact; however, these assumptions are not valid in mobile opportunistic networking environments. This results in unsustainable routes for nodes on their paths and poor forwarding decisions due to a lack of sufficient time for nodes to establish stable connections during their travels; therefore, delivery performance is also degraded as nodes become more mobile.
- **Security Vulnerabilities and Selfish Node Behavior:** Because of the lack of a central authority to manage networks, distributed networks are much more susceptible to many types of selfish or malicious behavior by nodes, such as the dropping of packets, the forwarding of only selected packets, and the injecting of false feedback into the network. Existing security mechanisms based on trust and reputation depend on trust evaluations based on delayed feedback and/or incomplete information. As a result, these types of security mechanisms are vulnerable to advanced types of attacks, and the lack of central authority makes it difficult to enforce cooperative behaviour among the nodes in a distributed network.

- **Inefficiency of Conventional Security Mechanisms:** The reliance of traditional cryptographic security techniques on centralized key distribution and key management makes them inappropriate for OppNets. Heavyweight security solutions are infeasible for mobile nodes, as they have limited computational power, storage, and energy resources, resulting in longer times for transmitting packets and higher latency, leading to lower performance of the network.
- **Insufficient Context Awareness in Routing Decisions:** Most existing routing strategies incorporate a limited set of contextual parameters, such as encounter probability or historical contact data. The most important factors for making these routing decisions, node stability, duration of contact, remaining energy, buffer usage, and cooperative behavior, are not considered. Therefore, forwarding strategies based on only limited information can produce less than optimal forwarding decisions and inefficiently use available resources.
- **Scalability and Resource Overhead Constraints:** Many of the existing routing and security solutions become very computationally complex and introduce a lot of communication overhead as the size of the networks grows and increases in density. They will not work in a practical, real-world deployment of large-scale opportunistic networks, where both scalability and resource efficiency are critical.

A complete solution should address Routing Overhead, Delivery Reliability, Selfishness Detection, Light-weight Security, and Adaptability or ability to adapt the protocol to changing conditions. In addition, a complete solution should also provide an efficient use of the network's resources. The current state of the wireless opportunistic network is a combination of multiple point solutions and requires a scalable design in order to best serve the needs of the network.

Proposed solution

This dissertation will propose an integrated framework to manage the challenges of routing efficiency, security, and privacy in opportunistic networks [132,133]. The proposed framework is based on the combination of adaptive routing that is stable-aware and

cooperative security through identity-based encryption to provide reliable, efficient, and secure communication for opportunistic networks.

- **Routing Efficiency Module (REM):** The Routing Efficiency Module's core component is the Stability Aware Spray-Wait Routing Algorithm with Capacity Evaluation and Dynamic Adaptation (STCESW-DSA). Node stability is determined through various contextual parameters, which include node mobility, encounter rate, contact duration, residual energy, and available buffer space, in order to evaluate the node's stability. The Routing Efficiency Module provides a method for dynamically adapting message storage and forwarding decisions based upon the stability of a node's connection and reduces the number of additional transmissions required while increasing reliability and overall efficiency of message delivery.
- **Dynamic Adaptation Mechanism:** The Dynamic Adaptation Mechanism gives Node J the ability to constantly modify the number of duplicate copies produced for each incoming message according to Current Network Condition and Resource Availability. By reducing the number of copies created for messages, and prioritizing more reliable nodes as opposed to those relaying messages with low priority, will decrease the instances of overload in the buffering of packets, as well as saving energy and decreasing the amount of time it takes for messages to be delivered.
- **Security and Privacy Framework (SPONS):** The integration of SORSI as part of the social-based opportunistic routing framework will enable greater security and cooperation among nodes. This can be accomplished by using the ESS to identify selfish nodes, as well as incentivizing and penalizing cooperative behaviour on behalf of other nodes, thereby ensuring reliable and consistent participation from all nodes involved with forwarding messages.
- **Identity-Based Secure Communication:** Using the HIBS framework, you can achieve end-to-end confidentiality, authentication, and integrity without having a centralized key distribution system or needing a Certification Authority. Messages

sent over the network are secured with the destination node's identity so that when they traverse through multiple nodes on their way to the final destination, those intermediate nodes will not be able to see or read any of the message content, as it will be completely encrypted.

1.4 Objectives

The major purpose of this research is to build, code, and test an integrated approach that improves the way routes are created, in addition to routing security and routing scale in opportunistic networks that operate in extremely dynamic and limited resources. The research will achieve these goals by implementing several specific objectives:

- To analyse existing routing schemes in opportunistic Networks(OppNets) in order to understand their design principles, strengths, and limitations under dynamic and infrastructure less environments.
- To classify routing approaches used in Opportunistic Networks based on forwarding strategies, network awareness, node mobility, and contact opportunities.
- To identify and evaluate suitable routing metrics such as duration, delivery probability, buffer occupancy, residual energy, and node stability for efficient data forwarding in OppNets.
- To compare the performance of selected routing protocols in opportunistic Networks using key performance indicators, including delivery ratio, latency, overhead, energy consumption, and buffer utilization.
- To study and review existing security mechanisms for routing in Opportunistic Networks, focusing on protection against attacks such as packet dropping, impersonation, and data tampering.
- Designing or improving existing secure routing protocols for opportunistic networks that provide assurance of the integrity of data, authentication of the sender and resilience to attack from malicious nodes.
- Review of mechanisms available to protect privacy within an opportunistic network, as well as the ways to conceal one's identity, protect the user's location, and to be anonymous in all situations.

1.5 Scope

The framework developed and presented within this document provides a model to assist in the development of routing and security solutions for Opportunistic Networks. The opportunistic nature of these networks creates difficulties in establishing an efficient route for the transmission of messages because of the store-carry-forward communication and intermittent connectivity used as the primary means of communicating within the network. The research conducted to develop this framework is focused on providing solutions to the obstacles faced in Routing Efficiency, Security, and Scalability, due to the extreme dynamics and the limited resources available within less traditional routing scenarios. In particular, the focus will include creating a Routing Mechanism that is Adaptive, Stable, and Environmentally Aware; therefore, reducing the Routing Overhead and Message Flooding while increasing the Delivery Reliability. To enhance decision making by Nodes, parameters related to Node Mobility, Time contacts remain together, Encounter Rates, Remaining Energy, Amount of Buffer Utilized, and Behaviours of Nodes working together were considered in a context-aware fashion. To secure the communications transported over opportunistic networks, we

address the need for Security and Privacy through the introduction of a Cooperation Aware Selfish Node Detection Mechanism and using Identity Based Encryption, which eliminates the requirement for centralised key management. For this reason, the Performance Analysis was conducted using the ONE simulator as a Testing Environment and used Realistic Mobility Models (RM) and Realistic Network Conditions (RNC).The performance metrics being measured for our proposed Framework included the Delivery Ratio, Overhead Ratio, and Average Latency compared against select existing Routing Protocols; thus, demonstrating an improved routing methodology. While this study focuses primarily on routing and security layers in opportunistic networks, it is important to note that it does not consider any physical enhancements to the physical layer or develop a blockchain based Implementation; nor does it test the proposed physical layer Developing Solution in a Realistic Physical Network. A key objective of this proposed solution is to create the

framework through which we can realize a scalable and efficient Communications strategy in Highly Dynamic Resource Constrained Networks.

Furthermore, regarding the areas of opportunistic networks that apply to both security and routing efficiency, the emphasis of this thesis is more heavily weighted towards routing and security as an integrated system to resolve some of the more challenging practical issues discovered during this research. The presented framework focuses on context-aware routing, allowing all nodes within an opportunistic network to make informed forwarding decisions based upon their assessment of connectivity, reliability and trust of other nodes rather than on pure connectivity alone. Providing a dual focus allows the system to reduce the effects of malice or selfishness of nodes on messages; therefore, providing the highest possible level of strength to maintain message integrity while enhancing the overall strength and resiliency of a network that is decentralized and highly dynamic.

Currently, the research only provides limited information regarding its adaptability and application within a narrow scope. Therefore, within its scope, it covers analyzing how adaptable the routing mechanism would be in different network conditions. For instance, in node mobility, a highly mobile node would not be a problem with the methodology that has been developed, as long as realistic models are applied. For instance, in various networks, including mobile networks and networks deployed in recovery operations and those deployed in vehicles, various simulation tools are helpful in carrying out research. Therefore, by using realistic mobility models in a tool referred to as one, a wide scope of applicability would be achieved. Additionally, it would cover understanding how various parameters, including contact time, frequency, and node energy, would play a role in ensuring its adaptability.

As far as security is considered within this scope, lightweight and decentralized security approaches can be developed, which can entail a particular solution based on a combination of cooperative awareness of selfish node identification along with identity-based encryption. This ensures that this particular framework is not obstructed, even in terms of being a lightweight solution, as there is no need for a centralized key distribution. Therefore, this is a promising solution as far as security is considered, especially in terms of being a solution that ensures the privacy of communication of sensitive information within the network.

Another important issue is to emphasize certain limits and boundaries of this particular study. Though this particular methodology emphasizes routing efficiencies and security improvements, it is important to note that hardware-level optimization studies, blockchain-based DLT approaches, and experimental studies conducted on actual physical-level networks are not within the limits of our manuscript. Also important are energy harvesting approaches and advanced physical layer routing optimizations, along with other routing protocols and layer optimization approaches. The approach and aim of this particular study are to enhance certain key performance metrics through measurable improvements in aspects like delivery ratios and latency.

Lastly, the scope of the work also aims to offer an opportunity for future development in the area of opportunistic networking itself. By showing the potential to increase network performance through the use of network awareness for both routing and security considerations for network stabilization, this thesis offers an opportunity for the continued development of more robust adaptive protocols for use in the area of opportunistic networking and the possible employment of more recent technology innovations, such as blockchain or machine learning. The framework with the proposed suggestions has shown an opportunity to develop three specific improvements with respect to the efficiency of opportunistic communication as a result of the solutions derived, which will improve the system as well as network performance.

1.6 Organization of Thesis

The research work described in this thesis has been broken down into several distinct sections in order to provide a systematic and logical presentation of the research. Each section focuses on a different aspect of the research, starting with a description of the research problem area, and continuing with an extensive review of prior studies relevant to the research area, a description of the methodology used, and an analysis of the experimental results, which will be followed by the conclusion and suggestions for future research on the topic. This structured format will help the reader to have a clearer understanding of the proposed solution, as well as create continuity between the various sections.

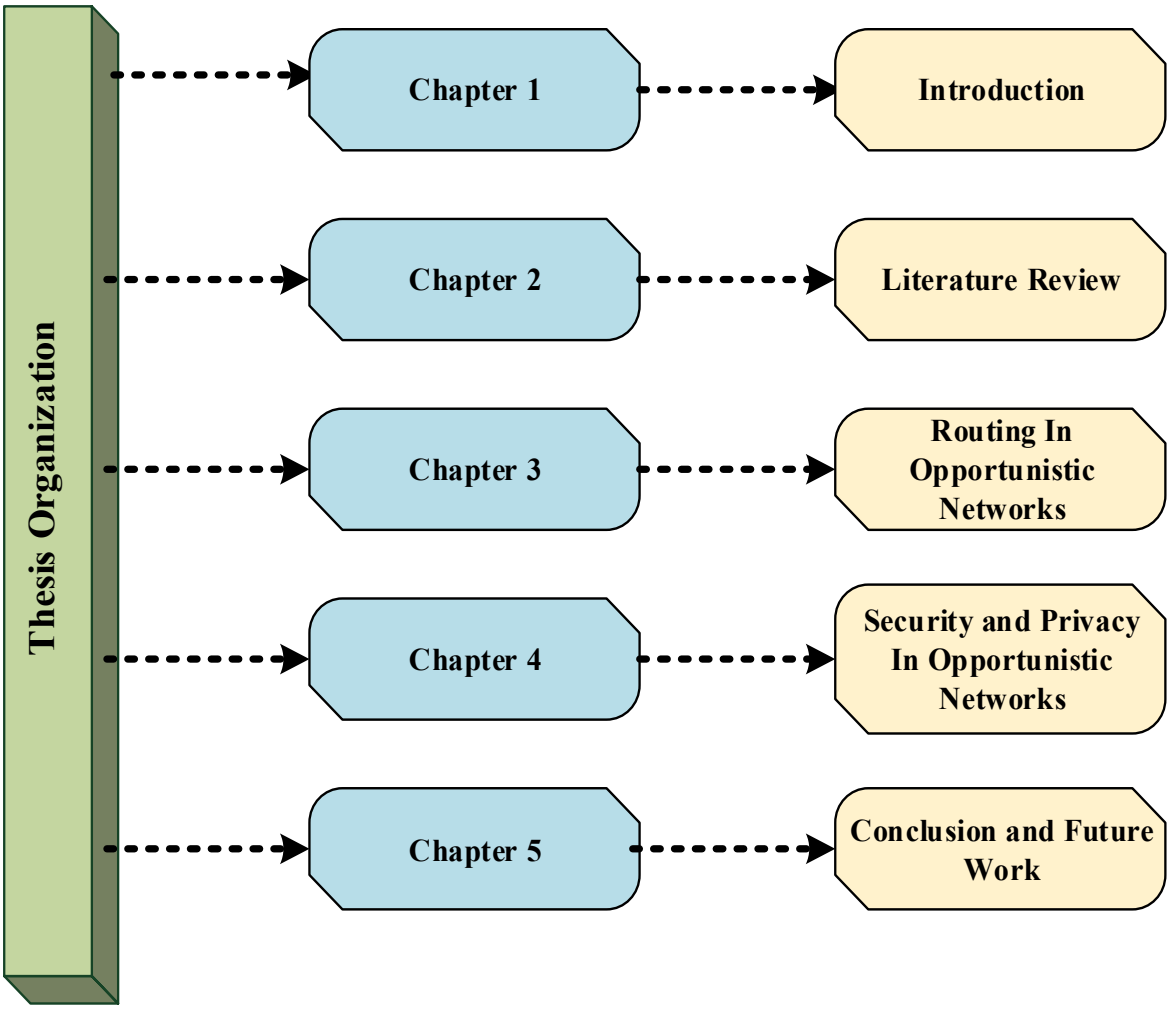

Fig1. 2 Thesis Organisation

- **Chapter 1:** In this Research Topic, as it pertains to Users / Customers of the Research's Background, the Potential User Group of this Study will be referred to as 'Opportunistic Networks'
- **Chapter 2:** This research is an Extensive Review of Existing Literature Relating to Research on Routing Protocols, Security Mechanisms and Mobility Models in Opportunistic Networks. It also identifies Areas of Research where there remains a gap and a Limitation with the current research approach.
- **Chapter 3:** In this study the proposed routing efficiency framework, including the stability-aware spray and wait routing algorithm with dynamic adaptation (STCESW-DSA). It will describe how the system architecture is designed, how the algorithm was created, and finally, how the simulation setup was created to evaluate the performance of the framework.
- **Chapter 4:** This study has the focus on security and privacy with regard to Opportunistic Networks. The chapter introduces the cooperation-aware security framework, which encompasses self-serving node detection (SORSI) and identity-based public key cryptography (HIBS), along with an experimental and comparative evaluation of the two frameworks.
- **Chapter 5:** The results and discussion of the analysis of the performance of the proposed framework through the evaluation of delivery ratio, overhead ratio, and latency. In addition, comparisons are made between the proposed framework and existing routing and security methods/techniques. This chapter concludes with a summary of the contributions to this thesis, the major findings of the research, and limitations to this research, along with consideration of further opportunities for research work within the field of opportunistic networking.

1.7 Summary

The chapter has discussed the concepts of Opportunistic Networks (OppNets) and the real-world research context in which these networks provide a method by which we can communicate in a very dynamic and infrastructure-less world. The unique features of OppNets are defined, from the lack of any predictable continuity in connectivity to the unpredictability of node movements, through to their lack of a centralised infrastructure and solutions for routing, security, and node mobility.

The impetus for the study is represented as a response to a number of significant identified problems: the inefficiency of current routing methods, excessive consumption of network resources, vulnerabilities in security procedures, lack of awareness of context, and problems associated with scaling the network to include more users. A concise problem statement has been created that defines the overall goal of this research as developing a single, adaptive, and resource-efficient framework, which improves both the routing performance and security of existing networks.

The thesis outlines a solution that includes a Stability-aware Adaptive Routing Mechanism (SARMs) to optimize routing decisions based on the state of a network, and a Cooperation-based Security and Identity-based Encryption framework (CSEIF) for data confidentiality and integrity[126,127]. This chapter establishes a framework for further research by providing objectives and a scope. The objective and scope will help to demarcate the boundaries of this research. The chapter concludes by presenting the organization of the thesis and giving a structured view of the coming chapters. The content of this chapter will lay the groundwork for the remainder of the thesis, which will include a literature review and the identification and development of proposed methodologies.

In addition, this introduction places importance on designing methods for routing and securing information within opportunistic networks that work well in an unstable and resource-deprived environment[128]. This introduction highlights the shortcomings of the currently developed methods; therefore, adaptive methods must be developed to effectively respond to extensive changes in how nodes behave, how nodes move, and node density

within a network. The proposed framework is adding routing efficiencies, stability awareness, and Security into one system rather than treating them separately.

This chapter emphasises that to achieve sustainable growth of networks, a key consideration is how to achieve an equal balance between increasing performance vs. scalability and energy efficiency. In addition, the increasing importance of opportunistic networks in real-world applications has increased the relevance of this research. Examples of such applications include disaster recovery, mobile social network sites, vehicle-to-vehicle communications, and military operations. All these areas typically do not have reliable physical infrastructure to use. Thus, the solutions proposed in this paper will be adaptable for different uses, while still providing adequate delivery reliability and security.

This chapter is intended to prepare the reader for the remainder of the thesis. This chapter presents an overview of the research question and the proposed solution. Subsequent chapters include an extensive review of the literature relevant to the proposed research area, the impact of existing research on this area, and the research design, implementation; and evaluation of the research methods used to develop routing and security frameworks. By detailing the rationale behind, goals for, and the limits placed on the research at the beginning of this thesis, this chapter provides a basis for the research presented in all subsequent chapters of the thesis.

Chapter 2

This chapter reviews existing research on routing protocols, security mechanisms, and mobility models in Opportunistic Networks. It highlights the evolution of routing techniques, examines key security approaches and their limitations, and analyzes mobility models used for realistic simulations. The chapter identifies major research gaps and motivates the need for an integrated, adaptive, and lightweight routing–security framework.

The chapter is divided into five sections which outline the various components of an OppNet. The first section (2.1) will provide an overview about routing protocols utilized in OppNets and how they can be separated by their forwarding methodologies and performance metrics. Section 2.2 reviews security measures such as cryptographic technologies, trust models, and privacy-preserving technologies. Section 2.3 looks at mobilization models and how to use these models to produce realistic simulations when generating networks. Section 2.4 identifies areas within the literature where there are gaps, such as lack of routing adaptiveness, security issues, and the lack of mobility simulations. In conclusion, Section 2.5 provides a summary of the findings and will make a case for an appropriate integrated, lightweight, and adaptive approach to close the gaps identified within the literature.

Background

“Opportunistic Networks (OppNets)” are an important way to communicate in highly dynamic, non-infrastructure environments where continuous end-to-end communications will not be totally guaranteed to exist. OppNets dynamically transmit data using intermittently established contacts among nodes that employ the store-carry-forward communication model to facilitate data transmission. Since node movements are unpredictable and each node can change frequently over time and operate in a decentralised manner, routing efficiency, support for security and support for realistic mobility models are significant problems that OppNets will experience. Therefore, extensive research has been conducted on OppNets to

develop solutions that improve data delivery reliability, reduce overheads and ensure secure communications. Opportunistic networking routing protocols have changed from basic flooding methods towards intelligent methods that are aware of context [15-20]. Current trust-based and reputation-based protocols use a contextual attribute and probabilistic assessment of node trust worthiness in order to prevent malicious nodes from acting maliciously. In addition to these two evolving categories of the routing protocol family, there are also a number of community based routing methods that exploit the relationship between nodes and group together those nodes with similar social behaviour to improve the efficiency of their forwarding decision making process. Yet another family of routing protocols is based on reinforcement learning and on using game theoretic strategies to model the environment and the dynamics of the routing protocol. These routing protocols implement a process by which routing strategies are adapted based on feedback from the network and any changes to the operational environment. There is also a number of adaptive clustering and Delay-Tolerant Network based routing protocol families which are designed to increase the probability that the payload will be successfully delivered while decreasing the amount of energy consumed. In addition, most routing approaches to opportunistic networks still experience high computational complexity, frequent interruptions in routing due to errors in the communication channel, increased latency, congestion in the buffers and decreased levels of scalability as the density and mobility of the nodes in the network increase. Security in OppNets is a significant issue because there is no centralized management, there is frequently an interruption in connectivity (which means the network will not be available to work), and mobile nodes have limited resources [21-25, 28]. The traditional cryptographic mechanisms that have been developed for security are not effective because they require complex methods of key distribution/management. Artificial Intelligence, Deep Learning, Trust-based Frameworks and Blockchain-assisted Security Mechanisms are being investigated in conjunction with each of these issues to improve Secure Routing, Attack Detection and Link Prediction in OppNets. There have been efforts to improve the reliability of delivery by implementing Social-aware Security Models and Community-Based Secure Routing Protocols, and reduce redundant transmissions [135]. However, the security solutions

currently available face significant obstacles, such as Inaccurate Trust Evaluation due to delayed feedback; Vulnerability to sophisticated attacks; Minimal utilization of the contextual features in developing Learning Model,; and Excessive Computational and Energy Overheads, which will limit the ability to utilize them in real-world OppNet environments. In conclusion, there have been important advancements in the areas of routing, security, and mobility modelling related to opportunistic networks in the literature. Unfortunately, there are a number of key issues that remain, including the challenges of intermittent connectivity, increased overhead for routing and security, limited adaptability to high levels of mobile user activity, and decreased awareness of the surrounding context [23,101-110]. Addressing these research gaps will require the development of integrated, lightweight, and adaptive design frameworks that will combine and optimise routing effectiveness, security strength, and dynamic mobility for new types of opportunistic networks.

The performance metrics obtained through evaluation have shown that the proposed integrated framework provides a significant improvement in the routing performance and security of an opportunistic network by increasing the routing efficiency of the network. The increase in delivery ratio illustrates that the stability-aware routing mechanism chooses the most stable forward path when routing packets in a highly mobile environment. The SECESW-DSA routing approach, which uses encounter history, stability metrics, and copy control to decrease unnecessary duplications of messages, allows for enhanced reliability of packets during end-to-end delivery [111,112]. Both the effective utilization of networks and the timing of delivery cost offer a novel base from which all consequently deployed opportunistic networks will have an improved chance of successfully achieving large-scale growth.

The latency analysis explicitly illustrates the effectiveness of the proposed solution. The lower average latency values tell us that messages arrive faster as a result of the use of efficient relay node selection and reduction in buffer congestion. Additionally, the ease of using the cumulative delivery probability curves shows that a larger percentage of messages, when compared to the traditional routing and security schemes, are delivered during shorter time intervals. This improved performance indicates that by combining stability awareness

with cooperative forwarding, delays from unreliable or selfish nodes that are usually the source of problems caused by message propagation in opportunistic networks can be mitigated [114,119].

Security and privacy in opportunistic networks are a priority for applications that include emergency response, military communications, healthcare monitoring, intelligent transportation systems, and so forth. Opportunistic networks face many risks of attack, such as packet dropping, impersonation, data modification by malicious third parties, Sybil attacks, and selfish nodes. Therefore, numerous lightweight cryptography solutions, identity-based security mechanisms, and trust-aware authentication methodologies are in development to fulfil this need while minimising the complexity of managing the keys used for secure data transmission [124,129]. However, the challenge remains to balance strong security guarantees with low latency and energy efficiency. Consists of a synthetic, non-realistic (or oversimplified) version. This makes it difficult to apply to the real world. With real mobility traces and socially driven mobility models, performance evaluations will be performed more reliably, and thus provide better opportunities for robust routing and security designs[141,142,154]. The need for mobility-aware adaptive protocols is even more pressing as protocols adapt to changes in node density, speed of movement, and contact duration so they can increase their efficiency (i.e., scalability) in denser and very highly mobile environments.

As a result of the incredible advancements opportunistic networking has made in the last 10 years, and with the increasing complexity associated with mobile environments and applications, there is an urgent need to develop routing frameworks that are lightweight, adaptive, and socially aware/secure. Future work should focus on reducing the computational workload of routing frameworks, increasing the accuracy of trust models, improving the resiliency of routing protocols to sophisticated attacks, and ensuring routing algorithms scale well in environments that have high rates of mobility [185, 189]. It is expected that by combining Social Routing, Advanced Security Models, and Intelligent Processing of Mobility into a single platform, users will be able to create a Reliable Communication Solution that is also secure with support for the next generation of Decentralised Applications.

2.1 Routing in Opportunistic Networks

A novel “Context-Aware Trust and Reputation Routing (CATR)” protocol for OppNet is proposed in this paper. It uses contextual factors and the probability density function to dynamically calculate nodes' trust and reputation values, resulting in effective data dissemination that effectively identifies and avoids malicious nodes. However, this proposed system can enhance the “performance metrics” prolonged by integrating the mechanism [193,196]. A “community clustering routing protocol” based on “information entropy in mobile opportunity networks (CREN)” is proposed in this paper. To split the “network nodes” into the “first clustering community”, the suggested protocol combines the “preselected initial clustering centre node” with the “K-Modes algorithm with supervised learning”. Then, built on the shift in “information entropy”, the communities with comparable traits are grouped together and combined. The “reputation opportunistic routing based on Q-learning (RORQ)” for effective routing is a reputation system used to classify and remove malicious nodes in a network by using a protocol that is based on “game theory”. Therefore, in an environment where malicious nodes are present, this method can more efficiently discover a routing path. According to the simulation results, the suggested approach could outperform other cutting-edge routing protocols in terms of routing performance[156,177,197].

However, the proposed method can have two difficulties in MANET; that is, network structure flexibility is high, and between routing, some interruptions enter as packet drop attacks. The “ACRP (Adaptive Clustering based Routing Protocol)” proposition. This “ACRP protocol” transforms the OppNet into a TCP/IP network and generates optimal clusters using the popular member-based adaptive dynamic clustering technique. With the help of this technique, nodes establish a lasting connection, which improves network performance and routing efficiency. This proposed model can decrease “energy consumption” and enhance the “network parameters”. A network paradigm called Delay-Tolerant Networking (DTN) was created especially to enable communication in settings where constant end-to-end

connectivity is unavailable or unreliable DTNs function in situations with sporadic connectivity[115,118], which are typical i remote locations, disaster areas, or space missions, in contrast to traditional networks that depend on steady connections. When a direct connection is not possible, nodes in DTNs store messages and forward them to other nodes using store-and forward techniques, which facilitate opportunistic data transmission [137-139]. The proposed "SCCM" is an efficient method of MANET security that ensures better throughput. The key concerns of this study are message confidentiality and message authentication. To "minimize latency and avoid packet loss", the WMECS protocol is used to select multiple routes during the forwarding of packets. After that, the original message is encrypted with ECC- based encryption before it is sent to the recipient [73, 74]. However, this proposed algorithm allows free movement both in and outside the network to the nodes in MANETs, which causes broken links, packet loss, and locations are frequently changed. The proposed novel algorithm for a variety of applications of MANETs, including edge networks with cloud solutions. We have adapted deep learning techniques used in routing procedures to artificial intelligence and decentralized blockchain technology. This type of communication path selection involved choosing the nodes with the best resilience, with the selection nodes being supplied by a network and technical factors. The ability of delay-tolerant networks to make effective use of available communication resources and gather real-time information about the status of nodes and messages through their constantly changing topology has presented difficulties when it comes to maximizing the operating efficiency of networks. To solve this problem, we have proposed an innovative routing protocol called Multi-Decision Dynamic Intelligent (MDDI), which will use double Q-Learning and node-to-node relationships and messaging to support better transmission of messages throughout the entire network [96, 97, and 99]. The MDDI routing protocol uses the entire network as a framework for Reinforcement Learning (RL), with each mobile device (i.e., each node) viewed as an artificial intelligence agent. In order for nodes to recognize the average latency for the entire network, every node is equipped with its own set of Q-tables; each Q-table contains Q-values where the value represents the forwarding action taken by the current node on behalf of a message in the forwarding process to its neighbour(s) (i.e., via a

neighbour)[39,58]. The average latencies associated with forwarding actions can also be used to relate to the average number of hops required to reach a target destination in the network, based on the resulting set of Q-values. Furthermore, it efficiently detected messages and selectively dropped messages from a buffer as the congestion arose and accordingly reduced the wasteful overhead. The applicability of the suggested paradigm extends to Internet of Things applications that are installed in difficult-to-reach areas, enabling the improvement of connection and effectiveness in these deployments [91, 93,202-207]. Using social user nodes to quantify user noise via AI-assisted techniques, a function optimization model is developed in a noisy environment. Several noise reduction strategies are derived from the data transmission context that will help to avoid losing significant information within the data itself. Additionally, different effective approaches to optimise the measured levels of noise are developed, and the utilisation of other effective means of evaluating adaptation between user nodes improves the user's ability to communicate with each other, diminishes the effects of noise, and increases the reliability of data transmission [66]. In table: 2.1 represent the limitations of Routing in Opportunistic Networks and Fig: 2.1 depicts Taxonomy of Routing in OppNets[209].

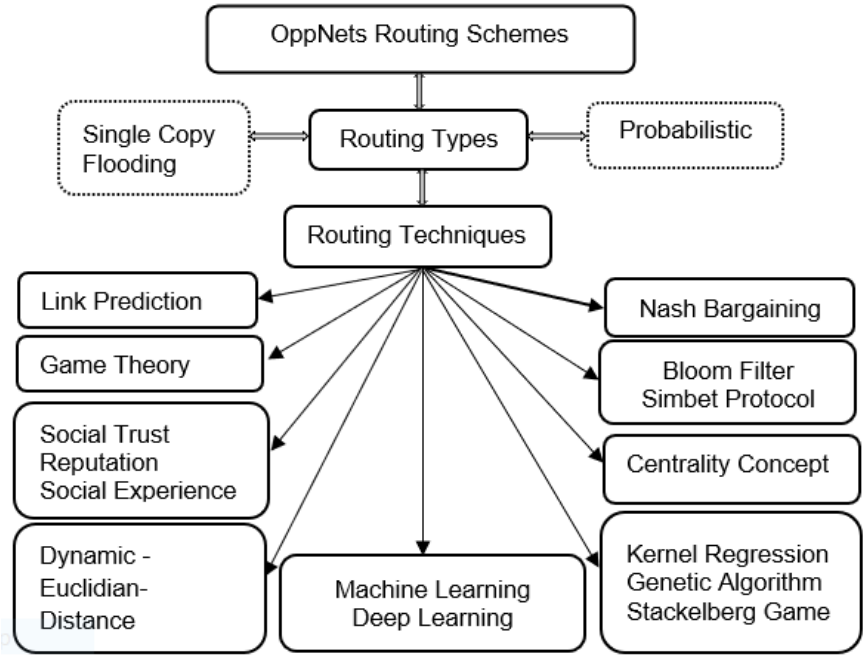

Fig2. 1 Taxonomy of Routing in Opportunistic Networks

Table2. 1 Limitations of Routing In Opportunistic Networks

Method	Key Idea	Metrics	Limitations
Epidemic Routing	Flood messages to all encountered nodes to maximize delivery probability	Delivery Ratio, Latency	Extremely high overhead, poor scalability, excessive buffer, and energy consumption
PRoPHET	Uses probabilistic delivery predictability based on encounter history	Delivery Ratio, Latency	Performance degrades under highly dynamic mobility and sparse encounters
MaxProp	Prioritizes packet forwarding and deletion based on the likelihood of delivery	Delivery Ratio, Buffer Occupancy	High computational complexity and control overhead
Bubble Rap	Utilizes community structure and node centrality for routing	Delivery Ratio, Overhead	Requires accurate community detection, sensitive to topology changes
SimBet	Combines social similarity and	Delivery Ratio,	High computation cost and limited performance in

	betweenness centrality	Delay	sparse networks
dLife	Considers time-evolving social interactions for routing decisions	Delivery Ratio, Latency	Requires long-term behavioral observations
SCORP	Uses social relationships and content interest awareness	Delivery Ratio, Overhead	Depends heavily on user interest profiling
Stability-based Routing	Selects relay nodes based on contact duration and stability	Delivery Ratio, Latency	Limited congestion awareness and copy control
Proposed STCESW-DSA	Integrates stability awareness, adaptive copy control, and resource constraints	Delivery Ratio, Overhead Ratio, Latency, Buffer Time	Evaluated primarily through simulation; real-world validation required

2.2 Security in Opportunistic Networks

OppNets are used to integrate the diverse “communication, sensing, storage, and other devices”. Conventional security measures are not always appropriate in DTN setups because of their unique characteristics. For instance, the sender must be aware of a recipient-specific encryption key in order to maintain end-to-end confidentiality using conventional encryption techniques. This paper suggests the attention feature fusion (AFF-LP) Link prediction model, which uses deep learning to automatically extract network characteristics. To excerpt the topological and temporal properties individually, the suggested model makes use of the “self-attention process” [40-45,]. However, the proposed model ignores node type, location information, etc., and simply takes the OppNets spatial-temporal information. Thus, add more data to enhance the model prediction performance. “HP-ECD” is a “heuristic prophet routing protocol” that relies on “asynchronous dormancy, cache optimisation, and energy balance”. To implement the node energy balancing technique, the “HP-ECD” first determines message forwarding welfares on several node parameters and message significance, as per Prophet. The “HP-ECD” then uses the node history data to create the message delivery list in order to implement the node cache optimisation method. A delay-tolerant network (DTN) that uses node self-organization to deliver network services. When the network topology changes at any time, and the communication link and special "store-carry-forward" functioning mode guarantee that it may conclude information transfer [143]. To keep improving the performance of “HP-ECD” so that, irrespective of the area’s size and node count, it can drastically lower the overhead rate. This paper develops an optimization multiple evaluation technique based on artificial intelligence. This method’s primary goals are to minimize data loss-induced information loss when reducing the noise and selecting the communication nodes in OppNets, which is used to maximize the data transmission efficiency and prevent the network congestion [46-50]. The timestamp approach is used to stop hostile nodes from altering the routing table during the feedback process, and the “trust routing table” is created based on nodes that were chosen. The security and dependability of transmission of data are

additionally enhanced by limiting the challenge of hostile nodes and carefully allocating network resources. The model is used to improve the quality of the network communication [191]. A social routing system called “Refine Social Broadcast (RSB)”. By using node interests and social behavior, RSB improves the network's message broadcast, increasing the likelihood of delivery while decreasing superfluous data duplication. Interest-based routing is united with the identification of influential nodes to transmit the information to the destination [173,174]. The goal of delay-tolerant networks (DTNs) is to facilitate communication in networks whose dynamic topology is unstable and moulded by mobile devices. In Fig:2.2 Depicts the taxonomy of Security and privacy in OppNets[209].

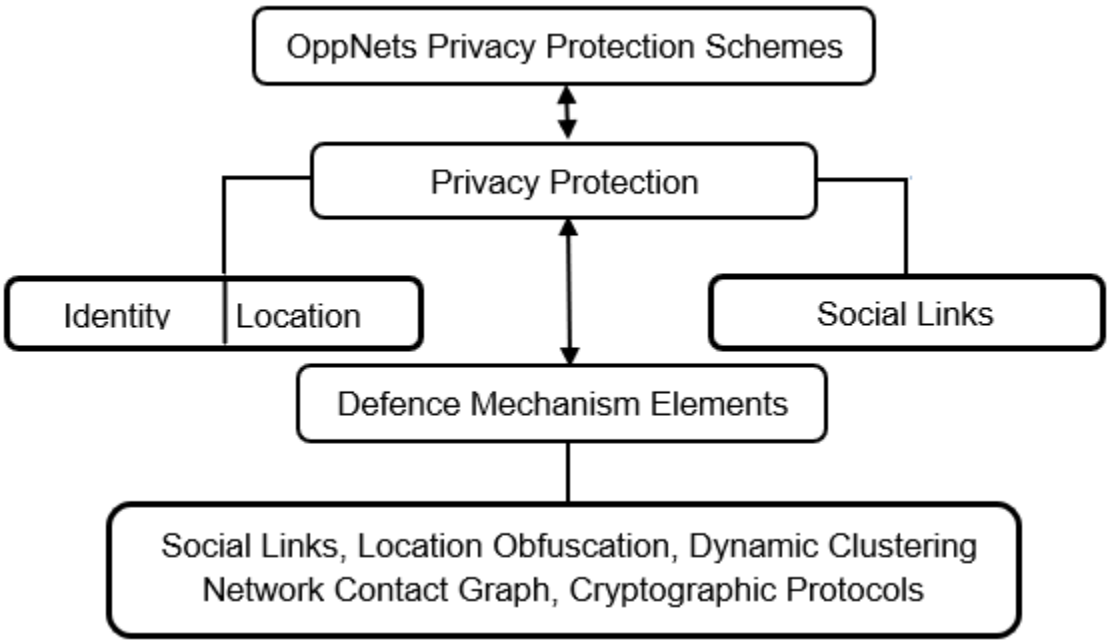

Fig2. 2 Taxonomy of Security in Opportunistic Networks

Figure 2.2 shows a proposed structured taxonomy of various security mechanisms deployed in opportunistic networks, categorizing some existing security solutions depending on their principles, layers, and objectives of operation. Security in OppNets faces a number of challenges attributed to connectivity, decentralization, and resource constraints in the network.

At this primary level, security solutions and techniques are categorized into three main categories, namely, Cryptography-Based Security, Trust and Reputation-Based, and Intelligence-Directed Security Solutions. The main aim of using cryptography-based security techniques is concerned with guaranteeing confidentiality, integrity, and authenticity of sent and received communication messages [51-55]. Despite guaranteeing strong security, this technique has been criticized for key management issues, which become a challenge in an infrastructure-less network that operates in a dynamic environment.

Trust and reputation-based security solutions make up the second major class of solutions within the taxonomy of ad hoc routing protocols. These solutions rely upon observations of past interactions, cooperative routing, and feedback from neighboring nodes. The routing nodes that are trusted most will be processed first. Routing nodes that present a high level of risk (selfish, compromised) are blacklisted from usage [56-60]. The use of trusted routes does produce a more robust system with respect to many internal risks like packet dropping and selective routing, this routing method doesn't always produce the desired results because of the time frame for receiving feedback, estimating trust levels, and the possibility of collusion. This taxonomy also points to Secure Routing Protocols, which incorporate security measures either directly or indirectly into routing. In this case, there is a combination of routing and other measures like authenticity and confidentiality, with respect to the secure routing of data. Secure routing helps to alleviate the chance of malicious engagement during routing, but generates further complexities [61-64].

One other important subcategory in the taxonomy is the category of "Privacy-Preserving Security Mechanisms," which seeks to ensure the protection of users' identity, location, and behavior information. In effect, "traffic analysis detection," "identity exposure prevention," and "location protection" are addressed in this category. Nonetheless, it is asserted that privacy-preserving measures may exacerbate processing complexity as well as affect routing efficiency in an adverse manner [80-84].

The branch of the Taxonomy Tree known as "AI and Machine Learning Security Mechanisms" is comprised of several methods, such as anomaly detection, predictive attack techniques, and link-based reliability estimation that can enhance an AI based detector's

effectiveness and adaptability. However, proper application of these AI/Machine Learning mechanisms requires a large volume of data and substantial computing resources to support the necessary computations. Blockchain is a mechanism that supports decentralised trust management and immutability in record-keeping. By providing a transparent view of all records and making records immutable, a blockchain provides resistance to tampering, but also adds considerable overhead in terms of processing power, storage, and energy requirements. These factors make blockchain unsuitable in practice for many opportunistic network applications.

In summary, Fig. 2.2 depicts that even though a broad spectrum of security mechanisms has been proposed in opportunistic networks, due to the inherent trade-offs of each category among the dimensions of security strength, resource consumptions scalability, and adaptability, this taxonomy conveys the need for lightweight integrated and context-aware security frameworks that can provide strong protection while remaining practical for opportunistic network real-world deployments.

However, in this proposed model, the routing algorithm performance can be improved. Communities in the opportunistic network are dynamically constructed based on the “weight distribution”, taking into consideration the “non-uniformity of communities”. An efficient data transmission technique based on SBM and community detection is proposed in this research to address the time complexity, hot transmission issues, and reduces overhead expenses. Low latency and low energy consumption will become more important needs for data transfer as the vast network of mobile devices grows [85-88]. It is crucial to conduct more research on lowering the temporal complexity of the routing algorithm in opportunistic networks. Then reasonably plan these jobs to perform them as quickly as possible. The proposed algorithm’s performance will be improved, and additional research into the security of data transfer in opportunistic social routing will be undertaken. In addition to the previously discussed methods of securing opportunistic networks, research must also address challenges arising from intermittent connectivity, lack of a centralized infrastructure, heterogeneous nodes, and high mobility. Traditional end-to-end security solutions do not perform well in these types of environments because there are frequent disconnections and

there is no lasting trust between nodes. Therefore, there has been a movement towards adaptive, decentralized, and lightweight security methods that can function effectively in delay-tolerant environments. One alternative method to traditional cryptographic security methods, gaining traction among researchers, is a trust-based security model. These types of security models assess the historical behaviour of nodes to determine if they are selfish or malicious, meaning they will drop packets, modify routing information, and disrupt the operation of a network. Trust or reputation values are used in opportunistic networks to select reliable relay nodes dynamically [90, 95]. Improving delivery performance and security are benefits of maintaining trust or reputation values based on historical forwarding behaviour. However, trust-based security models are susceptible to several issues, including but not limited to false recommendations, collusion attacks, and slow convergence of trust values, especially in sparse networks where the number of connections is minimal. As mentioned before, researchers need to address the problems of opportunistic networks caused by poor connectivity, lack of a centre for communication, heterogeneous node capabilities, and high mobility. Thus, adaptive, decentralised, and "lighter" forms of Security are being created to work in Delay Tolerant Networks (DTN) [159]. Trust-based Security models provide an alternative method for researchers to use instead of current cryptographic methods. Trust-based Security models evaluate the historical performance of Nodes to determine whether or not they have selfish or malicious intent toward other Nodes, e.g., dropping Packets, changing Routing Information, and disrupting Networks. Furthermore, Trust/reputation values are used in Opportunistic Networks to dynamically select appropriate Relay Nodes for forwarded packets. Trust/reputation values derived from prior forwarding behaviour of Nodes, used to calculate reliability, improve delivery performance, and Security of opportunistic networks. However, Trust-based Security models are subject to many pitfalls, including, but not limited to, False Recommendations, and Slow Convergence in trust/reputation values in Sparse Networks where the number of connections is low. Machine learning (ML) and artificial intelligence (AI) are key area of research for securing opportunistic networks (ONs). The purpose of these ML/AI approaches is to intelligently identify anomalous behavior, predict the occurrence of malicious activity, and adaptively

manage trust. Using spatio-temporal contact patterns and routing feedback from ON operations allows for improved accuracy in decision making [180,195]. Deployment of a learning-based security solution will need to be cognizant of the computational complexity, energy demand, and availability of training data, especially in resource-constrained environments. The rise of methods for decentralising cryptography, such as identity-based encryption and hierarchical identity-based schemes, as substitutes for public key infrastructure has great potential. In fact, decentralised forms of cryptography lower resource usage related to the creation, management, and distribution of certificates, making them more appropriate for opportunistic environments and delay-tolerant communication systems [100]. In table: 2.2 represented limitations of securities in Opportunistic networks.

Table2. 2 Limitations of Securities in Opportunistic Networks

Method	Key Idea	Metrics	Limitations
Centralized PKI-Based Security	Uses certificate authorities for authentication and encryption	Security Overhead, Latency	High overhead, poor scalability, single point of failure
Symmetric Key-Based Schemes	Pre-shared keys for secure communication	Encryption Cost, Energy	Key distribution and management complexity
Trust-Based Routing	Evaluates node behavior to establish trust levels	Detection Accuracy, Delivery Ratio	Vulnerable to false positives and collusion attacks
Reputation-Based Systems	Nodes rate others based on forwarding behavior	Detection Rate, Overhead	Slow convergence and manipulation risks
Incentive-Based Schemes	Rewards cooperative nodes using credits or tokens	Cooperation Ratio, Overhead	Requires secure accounting and credit management
Blockchain-Based Security	Uses a decentralized ledger for trust and incentives	Security Robustness, Overhead	High computational and storage cost
Identity-Based Encryption	Public keys derived from node identities	Encryption Overhead,	Key escrow issue at the private key generator

(IBE)		Latency	
HIBS	Hierarchical IBE enabling decentralized key generation	Security Cost, Scalability	Complexity increases with hierarchy depth
Privacy-Preserving Routing	Protects identity and location information	Privacy Level, Delivery Ratio	Trade-off between privacy and routing efficiency
Proposed SORSI-HIBS	Integrates trust detection with identity-based cryptography	Detection Accuracy, Delivery Ratio, Overhead	Simulation-based evaluation; blockchain integration remains future work

2.3 Mobility Models

A new mobility model in the field of "social network theory" has been created in this research paper to provide insight into social interactions between individuals. The topology of AODV and DSR protocols is characterised as being constantly changing regarding the physical locations of the protocols' users. Based upon this type of grouping, the model allows for the ability to collect and group individual users based upon social relationships, further grouping these hosts together by geographic/topographic regions. Each group is assigned a geographic location, and members of the group have the ability to participate in motion throughout a particular geographic region, depending on their individual social links, which can change based on time. The structure of an opportunity network of student nodes, plus their connection to smart devices within campus sites, constitutes a secondary form of opportunity network contained within the campus location [26, 27, 38]. Another way to look at the campus context is through how the individual student's trajectory depends on the interactions between other people at school. This research proposes a new method for predicting routes based on how students interact with one another by introducing a Markovian route prediction method for the prediction of campus routes. When a pair of nodes comes into contact with one another, the two nodes will exchange cache entries containing their respective distances and times to one another and use this information to compute the probability that they will come into contact with each other again. A measure of how closely connected nodes are to one another, or how central they are to each other, can be quantified through the degree of centrality of each node [219]. The level of importance of a message is defined in terms of the amount of time it takes for a message to spread and the energy consumed to send a message. Messages are stored and sent based on the utility value assigned to them. The purpose of this article is to provide a new fuzzy routing method for OMN. The new method, called FRIMF, uses the pairwise intercontact times to quantify the connection strength between any two nodes [121]. By using data from OMN nodes specifically the contact process, we have developed a bursty contact model instead of a random model, as well as a parameter that defines bursts in terms of duration to determine how "bursty" the dynamics is for each pair of

nodes' respective contacts within the overall system [136,168]. The variance of time between contacts and the mean duration of contact enable us to arrive at a single fuzzy routing metric used to implement the FRIMF routing architecture called closeness, representing the strength of connection between two nodes. In addition to creating a single fuzzy routing metric, to optimise FRIMF parameters for maximum efficiency, we also developed an optimal design procedure for generating membership functions based upon historical contact records for all pairwise node combinations[152,153]. In Fig:2.3 Taxonomy of Mobility Model in OppNets[1].

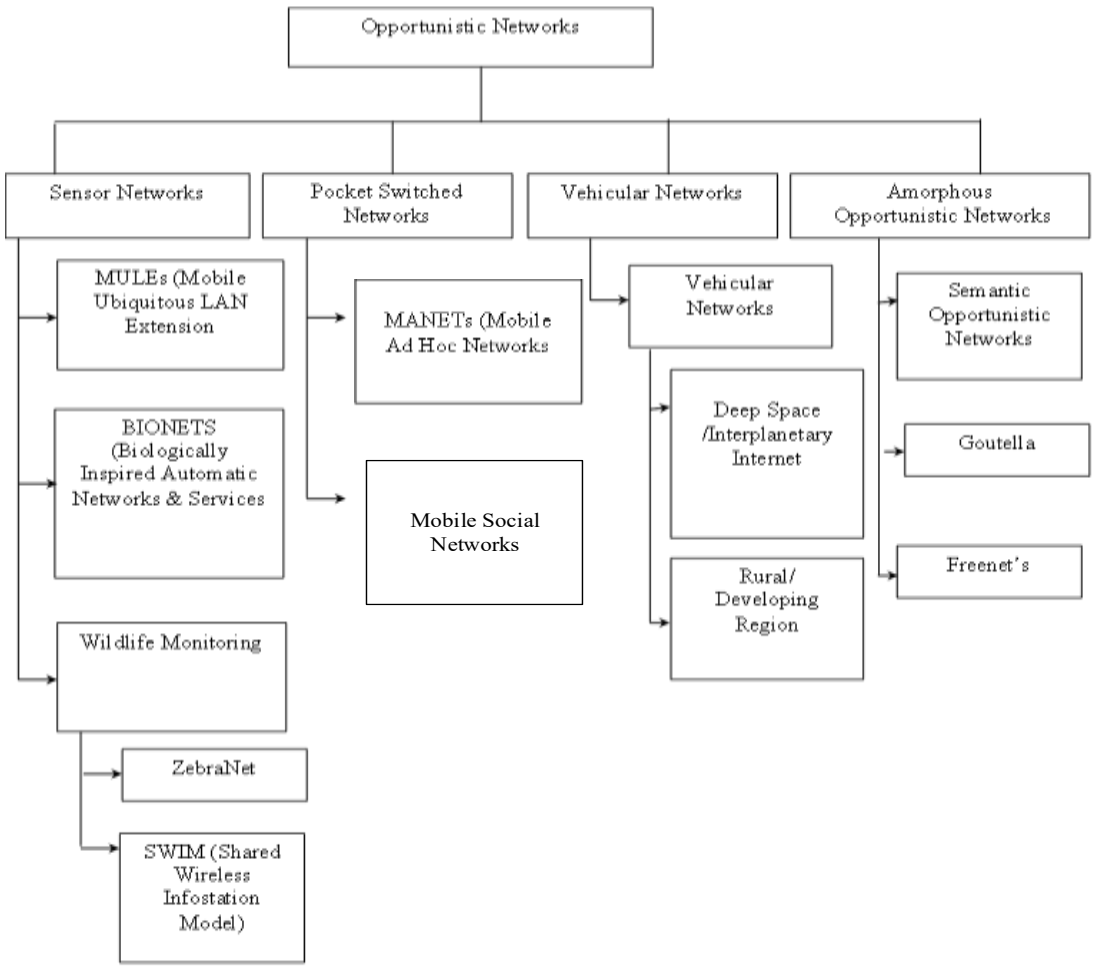

Fig2. 3 Taxonomy of Mobility Model in Opportunistic Networks

Figure 2.3 illustrates a broad taxonomy of opportunistic network mobility models by categorizing them into basic divisions: movement behaviour, social awareness, and temporal characteristics. In fact, in OppNets, the mobility model is an important factor because node movement is directly linked with contact opportunities, routing performance, and network connectivity.

Trace-based mobility models, conversely, are based on real traces that are collected from various users, vehicles, or other mobile entities, including sensors. Realism plays a great part in trace-based mobility models, as the traces show real situations and users. However, there exist various challenges, especially in large traces, large storage, and a lack of generalization.

Another significant category identified in the taxonomy is the category named Social-Aware Mobility Models. These models take advantage of social relationships in terms of user interactions. Here, the models consider social relationships such as the social community structures, the strength of friendships, as well as the encounter frequency in the simulations. Even though the social models have improved the efficiency of the routing through the increased social encounters by optimizing the simulations, the accuracy mostly lies in the ability to identify the social relationships.

Also within the mobility models section of the taxonomy is the inclusion of the Map-Based and Environment-Specific Mobility Model types. Under these types are the Campus Model, Urban Model, and Vehicular Model [175-178]. These types place a constraint or a boundary on the mobility of the node based on geography or the environment.

Another important category of network movement models consists of Markovian and Probabilistic Mobility Models, in which decision-making related to node movement is based on transition probability from a specific location. The network model captures temporal dependency in node locations while requiring a lot of historical data, leading to computationally expensive protocols.

Also, as shown in this taxonomy, Fuzzy and Bursty Contact-Based Mobility Models are identified. The latter are focused on modeling and understanding distributions of inter-contact times and bursty communications in opportunistic systems [181,182]. The effectiveness of these models is seen in enhancing short-term prediction but not in adjusting to long-term behavior and changing scenarios.

Overall, Fig. 2.3 shows that while various mobility models have been introduced to support opportunistic network simulations, there is, unfortunately, no mobility model that effectively describes and considers real-world scenarios with sufficient comprehensiveness. In fact, there are various advantages and disadvantages that arise with regard to real-world Scenarios, scalability, and adaptability with respect to these models. This shows that there is a great necessity to incorporate adaptable and aware mobility models to effectively support routing and secure communication scenarios in opportunistic networks.

2.4 Literature Gap

2.4.1 Limitations of Routing Mechanisms in Opportunistic Networks

- **Intermittent Connectivity and Dynamic Topology:** Frequent disconnections, rapidly changing network topology, and unpredictable node mobility significantly degrade routing stability and data delivery efficiency in opportunistic networks.
- **Insufficient Performance Optimization in Trust-based Routing:** Although trust and reputation-based routing protocols effectively identify malicious nodes, they suffer from increased routing overhead, higher end to end delay, and reduced packet delivery ratio due to the lack of holistic performance optimization.
- **Community-Detection-and-Cluster-Bases-Routing-Techniques:** The design and upkeep of community detection and clustering techniques for opposing networks requires a considerable amount of computational resources, particularly when utilizing over large geographical regions and continuous movement of the nodes in opposing networks. This means that the community-detection-and-cluster-based routing strategies will delay the growth of their routing methodologies. Given that opposing networks have both constant population densities and a constantly changing nature, and presents unique challenges when developing scalable routing methods.
- **Routing Interrupts in Reinforcement Learning based Methods:** Reinforcement learning driven routing mechanisms experience frequent routing interrupts and packet drop attacks as a result of unstable network structures and rapidly changing topology.
- **Limited Effectiveness of Adaptive Clustering under High Mobility:** Energy aware and adaptive clustering routing protocols rely on relatively stable links and long-lasting connections, which limit their effectiveness in highly mobile opportunistic network scenarios.
- **High Latency and Buffer Congestion in DTN Routing:** Store-carry-forward-based DTN routing models inherently introduce high delivery latency, buffer overflow, and excessive storage overhead during prolonged disconnections.

- **Limited Context Awareness in probability based Routing:** Routing strategies based on node meeting probability or visitation time utilize limited contextual information and fail to consider trust, mobility behaviour, and network conditions, reducing routing accuracy and robustness in adversarial or Congested networks.
- **Insufficient Assistance for Diverse Devices:** The majority of routing protocols for opportunistic networks assume that all nodes share similar energy, storage, and processing capabilities. However, when implemented in the real world, ON nodes consist of many different types of devices (e.g. Smartphones, Internet of Things devices, Vehicles, Sensors, etc.). As a result, current routing approaches do not adjust their forwarding decisions to take into account each individual device's capability; these results in unfair resource usage, prematurely depleted batteries or resources, and reduced total network life expectancy.
- **Inadequate Management of Congestion-Aware Routing:** Several routing protocols lack congestion awareness in their decision-making when forwarding messages. Because the protocols do not consider how much of the buffer is being used or how to manage the queue that is created in the router, there is likely to be a buffer overflow, packet drops, and repeated messages sent during periods of high traffic volume. This situation has a major effect on the performance of the routing protocol in areas where overcrowding and congestion are prevalent within a dense opportunistic networking atmosphere.
- **Restricted Resistance to Selfish Node Behavior:** Although various routing mechanisms exist to thwart bad actors, many do not consider the possibility of selfish nodes that may choose not to forward a packet to save on their own resources; therefore, selfish node behavior often goes unnoticed by current protocols that lack firm incentives or disincentives integrated into the routing process, permitting a selfish node to adversely affect the performance of the entire network without detection.
- **Reliance on Idealized Network Presumptions:** Many authors of routing-related literature assume things are perfect, including that messages will be transferred

perfectly, channels will communicate without error, and that clocks will be synchronized. This does not represent a true opportunistic network; therefore, performance statistics obtained from these assumptions are likely overstated, and they reduce the real-world performance of routing protocols when applied.

- **Inadequate Network Partition Resilience**: Opportunistic Network routing protocols do not adequately address the effects of long-term partitions on the stability of the network. The factors that contribute to this instability are not limited to the failure of the routing protocol itself, but also the failure to efficiently schedule and replicate messages, thus resulting in high latency and waste of network resources during the period of partition.
- **Lack of Lightweight Routing Options:** The common use of complex computational processes, large databases storing state information, and increased frequency of updates by advanced routing methods make them too heavy-weight to be used effectively on limited-resource networks such as Opportunistic Networks. In addition, thus far, there has been no successful development of lightweight methods of routing that provide equivalent levels of performance, security, and resource efficiency.
- **Insufficient Assessment Using Realistic Mobility Models:** Routing protocols are most commonly examined with synthetic mobility models, which produce irregular and inaccurate representations of how people and vehicles behave when moving through space and time. As a result, routing protocols can produce unreliable performance analysis and not account for the actual difficulties encountered in the real world regarding social dynamics, time-of-day mobility fluctuations, and location-based activities.
- **Inability to Adjust to Application-Specific Needs:** Predominantly, a generic forwarding method will be used for routing regardless of any given application. However, different types of needs from an Application level result in additional criteria relating to the reliability and latency of message delivery, as well as the priority for relaying data.

2.4.2 Limitations of Security Mechanisms in Opportunistic Networks

- **Lack of Continuous End-to-End Connectivity:** Without a stable connection between all devices that communicate over the Internet, it will be much harder to create and implement secure methods of communicating in an opportunistic network.
- **Complex Key Distribution and Management**: Security systems that rely on traditional encryption require the sender to know the recipient's key even before they send the message. Therefore, security systems based on traditional encryption cannot distribute and manage keys efficiently or effectively in a Mobile Node (MN) environment.
- **Frequent Link Breakage under Unrestricted Mobility:** Secure routing systems that permit mobile nodes to connect and send packets at will experience many interruptions, link failures, resulting in unreliable packet delivery and rapid changes in the location of nodes. Secure routing systems may offer enhanced security; however, they still do not guarantee a reliable means of transmitting packets securely.
- **Limited Feature Utilization in Deep Learning based Security Models:** Existing systems for detecting attacks and predicting links use deep learning based on spatiotemporal data while largely overlooking important contextual attributes such as node types, locations, and behaviour patterns of network participants that will significantly reduce accuracy of detection.
- **Inaccurate Trust Evaluation due to Delayed Feedback:** Existing trust and reputation-based security mechanisms using AI rely upon timely and accurate feedback; however, incorrect trust estimations are unavoidable due to delayed feedback from nodes and incomplete views of the network’s topology.
- **Vulnerability to Sophisticated Attacks:** Incorrectly estimating trust places the network at risk for many of the latest types of attacks, such as packet dropping, false feedback injection, and selective forwarding.
- **High Computational and Energy Overhead:** The use of combined AI and Blockchain security mechanisms adds a significant degree of computational

complexity, energy consumption, and scalability issues that limit their ability to be used in opportunistic networking environments where resources may be very limited.

- **Lack of a Centralized Trust Authority:** Opportunistic networks do not have a centralized network, nor any trusted authority, meaning consistent enforcement of security policies is challenging. Because there are no central trust anchors to support this network, authentication, authorization, and validation of trust becomes increasingly complicated. A large number of security mechanisms rely on a distributed method for evaluating trust, which has many drawbacks. For example, there is a potential for inconsistency between nodes, and updates to trust are delayed, as well as being vulnerable to manipulation by attackers.
- **Ineffective Authentication in Extremely Changing Settings**: In traditional authentication systems, the high frequency of mobility among mobile nodes and the short duration of contact between two mobile nodes hinder the performance of the traditional authentication systems. Many authentication systems require multiple message exchanges to complete the process of verification. In an opportunistic environment where the duration of an encounter is short, this is often not practical. Therefore, authentication attempts will fail, and attackers can impersonate victims.
- **Limited Ability to Preserve Privacy:** In addition to protecting confidentiality and integrity of data, most security systems do little to protect privacy. Identity exposure, location, and trackability via behavioural profiling create an added layer of vulnerability in OppNets. Existing solutions provide some degree of protection to users against traffic analysis and inference attacks, but do not offer sufficient protection to build user confidence and promote adoption of such systems in privacy-sensitive environments.
- **Inadequate Security Integration with Routing Choices:** Security mechanisms often operate as separate entities from routing protocols. This decoupling results in delays in identifying threats or providing an increase in the amount of resources needed to support routing, as an evil node remains part of the routing process until its trust has

been updated. The absence of integrated secure routing systems significantly hampers the capabilities of the network to perform timely reaction to a compromising situation.

- **Insufficient Defense against Collusion Attacks:** Most security architecture based on trust or reputation assumes that malicious nodes in the network operate independently. There is insufficient support in current security mechanisms for coordinated malicious attacks, such as collusion, or two or more malicious nodes working together to change a trust value or forwarding behaviour. This lack of support reduces the robustness of existing security solutions in inherently adversarial environments.
- **Over-Reliance on Past Conduct:** There are multiple security frameworks that assess the trustworthiness of nodes primarily based on historical interactions. Even though historical information is beneficial, it does not properly account for unexpected behavioral changes or an 'on-off' attack pattern. An excess of reliance on this information lowers the accuracy of detecting attacks, and enables advanced attackers to take advantage of the current system design that creates trust through accumulated interaction data/experience.
- **Inadequate Security Protocol Scalability:** As the size of a network increases, mechanisms for security that are dependent on frequent exchanges of trust, the need for the synchronization of the entire blockchain, or maintenance of a global state, will see their ability to scale decrease. Communication overhead, as well as additional storage requirements, degrade the overall performance and make large-scale opportunistic network deployments less feasible.
- **Limited Ability to Adjust to Resource Limitations:** Most advanced mechanisms for ensuring security rely on sufficient computational power, energy availability, and storage capacity to perform their functions. In a realistic opportunistic network, the majority of the nodes operate under strict limitations on their available resources. Existing mechanisms do not have any adaptive capability to alter the operation of a security mechanism to reflect changes in available resources.
- **Inadequate Validation in Realistic Attack Models:** In general, security mechanisms are evaluated based on simplified attack models and controlled simulations; however,

these evaluations do not account for the capabilities of actual attackers, who use adaptive, multi-phase, and stealthy approaches to perform their attacks. Evaluating security mechanisms against realistic threat models is a significant area for further research and is a major shortcoming of security mechanisms today.

2.4.3 Limitations of Existing Mobility Models in Opportunistic Networks

- **Resilience to Rapid Topological Adaptations:** Traditional mobility models using routing protocols like AODV & DSR do not adapt well when a lot of new connections or disconnections occur quickly. Because of how frequently topology changes, users experience unstable routing paths and reduced performance when using these protocols over dynamic opportunistic networks (DUNs).
- **Dependence on Social Relationship Accuracy:** Social network mobility models are primarily based around the proper identification and quantification of the social ties between individuals, but the fact is that these ties will evolve over time and cannot be effectively represented in a discrete way in any real-world situation.
- **Campus Mobility Models Limited Generalizability:** Mobility models developed for the campus environment that account for students' patterns of moving around will not likelybes general enough to be used successfully in many heterogeneous or large-scale opportunistic networks.
- **Scalability with Historical Contact Data Utilization:** Storing and processing historical contact data associated with every node pair adds an additional memory and processing burden which restricts the possibility of scaling in dense opportunistic network systems
- **Limited Adaptability of Bursty Contact Models:** Both Fuzzy Routing and Burst Contact-Based Mobility Models depend on historical inter-contact times to predict future mobility patterns; however it is likely that as networks continue to change and grow rapidly, they will become less accurate at predicting future behaviour based solely on historical data.

- **Insufficient Context-Aware Mobility Modeling:** Most existing Mobility Models do not include a user's context, such as the time of day, role within a system, environmental conditions, and Device Limits. The lack of context awareness within the Mobility Models will lead them to imitate real life inaccurately and decrease routing performance.
- **Inadequate Routing and Security Mechanism Integration:** Routing protocols are often created separately from, and without consideration for, either Mobility Models or Security Models. Because of this lack of integration, routing protocols cannot take full advantage of mobility predictions; likewise, Security Mechanisms cannot anticipate malicious movement patterns. Very few researchers have investigated Integrated Mobility-Aware Routing and Security Models together.
- **Inadequate Assistance for Diverse Mobility Trends:** Many mobility models assume that all nodes move in the same way, but actually, in reality, opportunistic networks contain many different kinds of nodes, each of which has a unique combination of speed, movement pattern, and pause time. Not taking into account heterogeneity in a mobility model limits both the realism and the use of existing mobility models.
- **Restricted Verification Using Actual Traces:** The majority of mobility models undergo validation through either synthetic logs (i.e., trace files) or small-scale The literature regarding the extent to which existing mobility models have been validated using authentic human mobility observations.

2.5 Summary

OppNets (Opportunistic Networks) use intermittent connections, and the Store-Cycle-Forward paradig, to offer users ways of creating communication channels in unstructured and rapidly changing settings with minimal infrastructure support. The unpredictability of nodes' movement along with the decentralized nature of OppNets and frequent breakages presents significant problems that impact the effectiveness of routing algorithms, provide ways to assure users of the security of their transactions and allow users to create realistic models of mobility. Over time routing protocols have transitioned from very rudimentary flooding techniques to the present use of Context-Aware, Trust-Based, Reputation-Based, Community-Based, Reinforcement Learning, Adaptive Clustering and DTN (delay-tolerant networks) approaches. Although the various techniques used have resulted in improved delivery probabilities along with fewer instances of duplicate transmissions, the means through which most existing techniques achieve these improvements result in substantial increases in the complexity of computing resources required (e.g., increased latency, excessive buffer overflow and scalability issues when transmitting packets in extremely high-density conditions. OppNets have a serious security issue because OppNet does not have centralized management of security from a trusted organization. Further complicating security is the finite amount of resources available on a node, as well as the discontinuity associated with links. The complexities associated with key distribution create a burden for traditional methods cryptography. Artificial Intelligence, Deep Learning, Trust-based Mechanisms, and Blockchain have been used to support secure routing, detect attacks, and predict the link. Existing solutions, however, have limitations in cases where time is an issue. These limitations include, but are not limited to delayed feedback leading to inaccurate trust evaluation, vulnerability to sophisticated attacks, only using a limited set of contextual features, and excessive computational and energy costs associated with using the existing solutions in a real-world OppNet. Mobility models have a significant impact on OppNet performance, as social-aware models, campus-based models, Markovian models, fuzzy

models, and bursty contact models are all utilized to create realistic movement patterns. Each of the above-mentioned models has both advantages and limitations in terms of their ability to adapt to rapidly changing topologies and their reliance on accurate social relationships. Additionally, each of the mobility modelshase limited utility for environments outside of their original environments because of their communication overhead associated with cache sharing and the amount of historical contact data collected needed for scalability. Through literature research, significant development has taken place regarding routing, security and mobility modelling in Opportunistic Networks; however, there are still some persistent issues. While there have been many improvements over the past few years regarding high-speed connectivity, user's still experience significant disruption when connecting to the network (intermittent connectivity). Additionally, routing and security overhead are still quite high (high routing and security overhead), which limits mobility. To address the gaps identified, the need exists for the creation of integrated, lightweight, and resourceful frameworks that incorporate a combined optimisation of routing performance, robust security and mobility awareness to support reliable and secure communication within future opportunistic networks.

A careful analysis of the interdependence of routing, security, and mobility illustrates that any improvement in one area alone will not be sufficient to improve overall performance. A coordinated approach to developing routing solutions needs to combine information regarding route contact opportunities with information regarding trustworthiness, resource availability, and mobility. Current solutions that treat each of these areas as separate have resulted in fragmented solutions that are not capable of functioning effectively under the real-world conditions of opportunistic networks, including a high degree of mobility, limited connectivity, and limited resource availability.

Additionally, several presently existing strategies have been tested in a controlled simulated environment using reduced or simplified assumptions related to node behaviours, mobility patterns, and attack models. Simulation evaluations for these strategies confirm their theoretical performance improvements, yet are unable to model the complexity and unpredictability of actual environments. The gap from simulation to implementation has

limited the ability to apply existing solutions and emphasises the need for frameworks validated via realistic or representative mobility patterns, heterogeneous device capabilities, and adversarial scenarios.

Another significant finding in the literature is that there is no evidence of adaptive systems that will effectively deal with quickly changing network conditions. Routing and security mechanisms are unable to effectively adapt to changes in node density, traffic load, and mobility because of three limiting factors; first, they rely on static parameter sets; second, they operate on a defined threshold; and third, they evaluate trust over a predefined time period. If you design an adaptive and learning-based routing or security mechanism so that the overhead of computation will not be excessive, these mechanisms may be very promising avenues for developing a mechanism that is more responsive and less dependent on computation than is currently possible.

Moreover, due to the limited use of contextual intelligence, the existing OppNet solutions aren't as effective as they could be. Using contextual characteristics like patterns of movement over time, how people interact socially, how much space is taken within a buffer, how much energy is still in the battery and previous co-operational behaviours, will give an insight into how to optimise routings and enforce security. However, being that currently used frameworks are employing only a small sample of these contextual characteristics, decision-making processes are incomplete and are not able to support reliable operations under conditions that are either highly congested or where there are malicious agents involved.

A comprehensive review of the literature indicates that there exists an imminent requirement for scalable, context-aware, and resource-efficient next-generationn opportunistic networking frameworks that combine intelligent routing techniques withlow-latencyy Secure Business Intelligence practices and realistic user mobility awareness for reliable data delivery in extreme network dynamic scenarios. The solutions identified will form the basis for the research supporting the design, development, and evaluation of an integrated framework that will enhance routing efficiency; augment security; facilitate

Adaptability; and improve the overall end-user experience within highly-dynamic opportunistic networking environments.

The research currently published indicates that in many cases, energy efficiency and resource awareness are treated as secondary goals in designing opportunistic networks. Since nodes in OppNets usually have limited battery power and limited storage space, inefficient resource usage will contribute to reduced network life and lower reliability of all messages sent within OppNets. A number of routing and security processes are not set up with an adaptive mechanism to control how often a message is replicated, how frequently a node is evaluated for trustworthiness, and how strongly a node will enforce security on its own resources. Consequently, some nodes are needlessly consuming large amounts of energy and being exhausted far sooner than they should have been.

In addition, there is a major limitation of the existing literature regarding the need for heterogeneity among application needs. Today, opportunistic networks are being utilized for many different types of applications, including but not limited to emergency management, vehicle communication, health monitoring and social media distribution. Each application has its own set of requirements (e.g., latency tolerance, reliability, privacy, data priority, etc.) and so each will require a different type of solution. However, the overwhelming majority of solutions currently available to users employ the same generic (one-size-fits-all) approach which can lead to a lack of flexibility and a diminished ability to effectively support applications across multiple fields of use.

Numerous author´s describe in their literature that achieving a balance between Robustness and Lightweightness is one of their greatest challenges. Deep Learning, Blockchain, and other advanced methods of Complex Trust Computing can significantly increase the security of opportunistic systems, as well as improve the predictions of the node´s movements; however, they also add significant overhead (in terms of computation, communications, and energy) to the system. That limits the viability of these methods within real-time opportunistic networks; therefore, there is a need for methods that are simple, yet sufficiently effective to guarantee acceptable levels of security and performance.

There is also inadequate cooperation between the layers of routing, security, and mobility in an OppNet, meaning that decisions made on one layer often contradict the goals of another layer. Examples of such contradictions include redundant transmissions at the routing layer, delayed identification of a security threat at the security layer, and inaccurate predictions regarding mobility at the mobility layer. Although cross-layer optimization has not yet been thoroughly explored, the potential for achieving a higher level of performance in an OppNet by enabling all layers to share information and optimize it together represents a promising area for future research.

Even though considerable advances have already been made in the area of reactive networking, much work remains to be completed regarding the development of appropriate methods for managing scalability, flexibility, security, and realism. The results presented here will inform further investigation aimed at developing a comprehensive, context-sensitive, resource-efficient platform that includes mobility features, security measures, and routing elements in a cohesive way, providing reliable, secure, flexible communication to end users in strategically placed scenarios with unpredictable resource limitations.

Chapter 3

This chapter introduces the STCESW-DSA routing framework for Opportunistic Networks, designed to improve delivery reliability while reducing routing overhead under dynamic and resource-constrained conditions. By using stability-aware, context-based forwarding and adaptive message replication, the framework enhances routing efficiency and scalability. Simulation results using the ONE simulator demonstrate significant improvements over existing protocols in delivery ratio, latency, overhead, buffer usage, and energy consumption.

In Chapter 3, we define the approach we take in Section 3.1 by listing out the methodology of how we develop the Routing Efficiency Module (REM) and stability-aware forwarding method, followed by an evaluation of the algorithm in Section 3.2 (STCESW-DSA), which describes in detail the time and space complexity of the STCESW-DSA algorithm. Also included is an explanation of the experiment which was conducted using the ONE simulator in Section 3.3 along with the parameters and configuration used for the simulation. Section 3.4 will present the comparative analysis of the results and performance of the STCESW-DSA compared to other routing protocols. Section 3.5 summarises the main conclusions and contributions of the overall routing framework proposed in this chapter.

Routing in Opportunistic Network

A significant challenge faced by routing in an opportunistic network is that opportunistic networks do not have continuous end-to-end connection, so routing has to be accomplished with an unpredictable, dynamic network topology and limited node resources, as well as with an unpredictable level of node mobility. Additionally, the routing paradigms used in

opportunistic networks are entirely different from routing in traditional ad hoc and infrastructure-based networks. OppNet routing uses a store-carry-forward concept, where nodes hold onto data until they reach a point when they can send it to another node (opportunity). Routing decisions must be made based on current and future connections to other nodes, without knowing when the next connection will happen. The classification of the Routing Protocols of OppNets can be best described by the amount of Network Knowledge they contain [161]. Using Flooding Routing Protocols, like Epidemic Routing, gives the best chance for delivery by sending copies of the message to all Nodes that are on the path of the message, or discovered. However, despite being the most effective at increasing the Delivery Ratio of a message, Flooding Routing Protocols create excessive amounts of Energy, Buffer and Overhead use, making them unsuitable for use in resource-limited environments. This has been addressed with the use of Quota Based Routing Protocols, like Spray and Wait, which attempts to provide a good delivery rate while minimizing the number of message copies that are created to balance Delivery Rate and Resource Utilization [160,162,163,157]. likely to reach the destination. Routing strategies are critical in the field of Opportunistic IoT (Internet of Things) as they determine how well an opportunistic network transmits data, and they affect the ability of the network to operate efficiently when there is unbalanced transmission efficiency and security [171]. This document describes a Hybrid Opportunistic IoT Secure Routing strategy based on node intimacy and trust values HI Router. The HI Router hybrid opportunistic IoT routing strategy calculates each node's node intimacy and trust value from these two factors. All message forwarding actions will occur on the intimacy and trust value between nodes. The introduction of massive quantities of multimedia big data (MBD) in the last few decades has created many difficulties for effectively engaging with the virtual era with the increasing ubiquity of Wireless Internet of Things (IoT). And as a result of the increased number of communication protocols and cost efficiency offered by Mobile Ad Hoc Networks for IoT (MANET IoT), it is becoming more popular. The experimental results indicate that using the HI Router algorithm improves message delivery rates and reduces the overhead rate of opportunistic Internet of Things networks with dense nodes and regular node-to-node interactions. While prediction-based routing does improve efficiency

compared to using a flooding method to deliver messages, there are many cases in highly dynamic or sparse networks with unpredictable contact patterns where prediction-based routing could potentially perform poorly.

The proposed energy-aware and trust-based routing protocol TAGA for wireless sensor networks is based upon Adaptive Genetic Algorithm. It aims to minimize data transmission energy consumption as well as combat Ridiculous, Routing Attacks and Special Trust Attacks. Machine learning and deep reinforcement learning-based routing solutions have recently come to the forefront of academic attention because they enable flexible routing policies that learn to adapt to changing conditions. Opportunistic networks create new ways to connect devices without having central infrastructure or an established way of connecting. Devices that can be carried by individuals, or that can be embedded in places like cars or buildings, can relay messages to other devices within their communication range. The most significant challenge facing network operators is the ability to determine the optimal route for a message while maintaining the privacy of both sender and receiver. Finding the right network parameters for node localization with the appropriate amount of accuracy in a timely manner during the setup process for a wireless sensor network can be extremely difficult. Network resources and routing protocol manipulation creates many types of routing attacks that can potentially affect both accuracy of localization and the level of service provided by a wireless sensor network, for example wormhole attacks, Sybil attacks, Blackhole attacks and replay attacks. To resolve this issue, we developed a novel routing algorithm, which uses a cluster-based approach to improve the performance of the overall network, while minimizing the amount of transmitted message traffic and allowing cloak-like techniques to hide identifying information from others attempting to connect with a network node. Selecting a routing protocol is one of the most critical considerations when considering how to safely route data packets to their destination with minimal overhead due to the inherent resource constraints of sensor networks. As such, many researchers have worked to provide the best routing solutions for wireless sensor networks; however there remains much more work that must be completed before optimal routing solutions are developed. The learning solutions will determine the best forwarding strategy by taking into consideration

many factors including buffer occupancy, contact time, mobility patterns, and available energy. Three elements that were considered to identify SNs in the network considered to be malicious were Forwarding Rate (FR), Response Time (RT), and Delayed Transmission. The proposed routing algorithm, Social Route, is an opportunistic routing protocol that also utilizes the relationship of individual users' social links, rather than routing information through communities [35-37]. We also evaluate using static relays placed in high traffic areas and their impact on message forwarding, which can also be aided through the use of a dissemination profile based on message content and priority. A routing mechanism was developed which will provide real-time, energy-efficient delivery of data from SNs to BSs, with the ANs serving as "relays" for delivering data. Data will be reliably and securely delivered using RSA technique. Using a learning-based solution for routing provides higher accuracy in decision-making and allows continued scalability. Due to their dependence on mobile nodes, OppNets are subject to frequent intermittent connectivity, fragmentation, and extended delay paths, therefore traditional routing practices for end-to-end connectivity can't be employed with the OppNet. Conversely, OppNet routers will use the SCF approach so they can transmit packets created by the Originator to the Final Destination sequentially (hop-to-hop). However, based on the learning process, the learning-based routing solutions may face computational complexity which can influence the speed of routing operations as well as convergence of the learning process. Even with all of the advances made to date, open research challenges still exist with regard to routing in OppNets; these include scalability when dealing with large-scale networks, energy-aware forwarding decisions, security-aware routing decisions, and Quality of Service optimization. Future routing solutions should incorporate advanced intelligent prediction and lightweight automatic learning methodologies along with optimization across multiple layers to facilitate reliable and effective data delivery in future generations of opportunistic communications environments. Opportunistic social networks[31-34] have been designed for transmitting data during high levels of congestion in 5G mobile networks; therefore, they are frequently used for improving transmission performance in these networks. Since an increased number of people downloading large files typically results in duplication of the data, this can negatively impact the quality of data

transmission. Therefore, the authors introduce a user-optimised scheduling method for data transmission based upon the idea of edge-community service available through opportunistic social networks, referred to as ECSUO. In order to develop an edge community service model (ECSUM), the authors incorporated mobile edge computing into an opportunistic social network (OSN). To this end, they constructed two separate schedules that allow for the identification of the most appropriate service request based on a variety of criteria (e.g., time, cost, priority) and coordinated all the schedules based on multiple factors that are subject to change over time. The results of this research demonstrate that ECSUO outperformed the existing classical algorithms used in opportunistic complex networks for a wide range of quality-of-service parameters and that this approach can be successfully extended to other types of service transmission models. Store-and-carry Forwarding methods are typically utilized in OppNet protocols, where each node keeps messages in their local memory and sends them further when an appropriate opportunity arises. TCP/IP Routing Protocols aren't well suited to the frequent disconnections and fragmented networks seen in many Delay Tolerant Networks, creating major challenges when attempting to use TCP/IP Routing Protocols over DTN channels. While DTN Routing Protocols are quite effective in highly fragmented Networks, they have high mean delivery delays, low Delivery Rates and produce more unnecessary overhead by utilising store-and-forward techniques and opportunistic Forwarding than TCP/IP Routing Protocols. Thus, by establishing a Cluster Based Routing Protocol as a substitute for the usual store-and-carry forwarding mechanism, the Delay Tolerant Network can be transformed into an inherently more connected structure supporting TCP/IP Protocols. The various clusters that may have overlapping nodes may also be disjoint from one another. Within each cluster, one node (the Cluster Head, or CH) has been designated to manage routing activities and therefore eliminate the member node overhead while simultaneously improving system efficiency. Clustering also introduces variable clustering/node to CH relationships leading to node to CH re-clustering and re-association in a clustered MANET; therefore an effective and efficient routing protocol must be employed in order to provide the best path options from any one node within a cluster to other nodes in the network. In defining how to partition the nodes (or entities) of an opportunistic network

into different community structures, we first determined what is meant by 'community' by using the distribution weighted nodes.

Link prediction remains a highly discussed topic in the field of Evolutionary Networks. Although many models have been developed to date, they implement a stacked architecture that feeds the topology information captured by the network into a time series model. The problem with this approach is that it adds noise to the network of which the temporal feature extraction process relies heavily upon to create an accurate representation of the temporal feature space - thereby making it difficult for the model to predict correctly. To address this, we have developed the AFF-LP model for predicting links based on attention mechanisms to perform feature fusion based on what has already been established in Computer Vision (CV). Based upon Deep Learning, this model will allow us to automatically extract all relevant network characteristics and incorporate them into the link prediction process. The Prophet routing protocol most probably works with the Mechanism Energy Balancing Technique, Cache Optimisation Mechanism and Asynchronous Dormancy Mechanism to produce HP-ECD - heuristic Prophet routing protocol based on energy balancing and cache optimisation through Asynchronous Dormancy. This paper has developed a Community dynamically updating mechanism to find the most effective Nodes in the community using the Social Attribute and Information Entropy of each Node. We have provided simulation evidence that our Community updating algorithm performs better than existing Classic Routing Algorithms in terms of success rate transmissions, lower transmission delay, and lower routing overhead. Campus opportunistic networks operate within campus areas and enable nodes students and teachers to communicate between themselves and utilize handheld mobile devices (HMDs) to connect. Nodes of a campus opportunistic network generally consist of students and instructors who are using HMDs. In the opportunistic social network, we are first considering how to divide nodes into multiple distinct communities based on how to construct communities in a dynamic environment based on the distribution of node weights. The advent of 5G networks has seen new modes of high-speed communication emerge. These have created issues that require solutions through appropriate Opportunistic Social Routing methods. 5G network development has created new

modes of high-speed communication that have created problems for which appropriate opportunistic socio-routing solutions must be found. Routing process resilience is one of the most difficult parts of data transmission over mobile networks without an underlying infrastructure. Presently, routing protocols provide routing through the shortest communication path, which in some cases can be insufficiently resilient when compared to alternative paths for mobile network-to-cloud communications. Malicious nodes are capable of causing disruption to the communication path via routing through malicious nodes or nodes that are in a poor technical state. This paper proposes a solution for mobile ad hoc networks that provide both direct connectivity into the cloud as well as connectivity to the cloud via routing with decentralized blockchain technology and artificial intelligence.

3.1 Proposed Methodology

In OppNets, there exist a number of protocol performance-related problems such as message flooding and high overhead. To resolve these limitations, this research proposes a combined algorithmic and mechanistic approach that will provide efficient routing and improve the effectiveness of communications in an opportunistic network. This proposed work is being referred to as the Routing Efficiency Module process**.**

The Routing Efficiency Module (REM)'s proposed design is a lightweight, flexible framework that will maximise routing performance by reducing Replication of Messages, Routing Overhead and improving Reliable Message Delivery during Intermittent Connections for Opportunistic Networks. The new routing methodology includes integration of Social Awareness, Trust Evaluation and Mobility Context to the process of determining a route for forwarding messages, allowing nodes to create intelligent forwarding decisions during opportunistic encounters.

The REM framework allows communications between individual devices to be performed using a store / carry / forward communication methodology, as opposed to traditional flood-based methods, in which messages are propagated to all nodes regardless of their relevance to the specific message being forwarded. The framework only allows for specific nodes to be chosen for message forwarding based on a variety of metrics, which will be evaluated dynamically, including: Frequency of Encounters, Historical Co-operation, Buffer Availability, Residual Energy and Moving Patterns. Therefore, by using these contextual factors to determine which nodes are most likely to carry forward messages, REM reduces the number of times messages are sent to nodes without a good chance of reaching their destination.

A mechanism that uses trust-based forwarding to assist in managing malicious and self-serving nodes has been developed as a result of this work. All nodes keep a record of their own trust scores regarding the nodes they have encountered; this score is revised as the node

observes the other node's forwarding behaviour and receives delivery acknowledgements from those other nodes. In time, nodes with low trust scores are less frequently included in the forwarding process, resulting in fewer dropped packets and a more stable overall network reliability. Since there are no centralised authorities or complicated key management associated with this process, the autonomous trust-based evaluation system can operate successfully in very fluid OppNet environments.

To increase route stability throughout the network, the proposed methodology has also integrated a mobility-aware routing mechanism. By studying the historical duration of contact, interval between subsequent contacts and patterns of movement, the REM framework can provide predictions of the likelihood of future contacts. The REM framework will prioritise nodes that exhibit higher levels of mobility stability, which will therefore reduce the frequency of routing interruption or failure due to sudden changes in network topology and, increase overall route performance during high-speed movement.

The Adaptive Message Replication Mechanism in the Routing Efficiency Module has a dynamic message replication strategy that allows for controlling network overhead and buffer congestion. This strategy allows message replications to be changed based upon current density of messages in the network, current state of occupancy of all network buffers and the urgency of the message to be delivered through the network.

In addition, the proposed methodology uses a design principle of Cross-Layer Optimization; that is, that routing decisions are influenced by trust, mobility and resource awareness (i.e., the location of the sender, the number of hops to reach the destination and the available resources). The Routing Efficiency Module has been designed to support a scalable, computationally efficient and robust solution to supporting an evolving network infrastructure. The effectiveness of the proposed methodology will be evaluated in simulation using a standard simulation tool for Opportunistic Networks and compared against traditional routing protocols based upon delivery ratio, latency, overhead ratio and energy use.

A. Routing Efficiency Module (REM)

The proposed STCESW-DSA is Stability–Aware Spray and Wait Routing Algorithm using Transmission Capacity Evaluation and Dynamic Adaptation. This method evaluates every node's stability to maintain a connection and successfully, messages can be forwarded based on metrics such as "mobility node, contact duration, residual energy and buffer size". The message forwarding can be chosen based on where nodes can have high stability scores. So, this can decrease the unnecessary transmissions and ensure reliable delivery. Often, the conditions of the network can be changed because of the mobility node and intermittent communications. The DSA mechanism helps to dynamically modify the amount of message copies and decision forwarding based on the current stability of the network. When network circumstances are not stable, the system can decrease the message loss and adjust by selecting the most stable relay nodes. Otherwise, spread fewer copies. It ensures decreased latency, increased delivery ratio and achieves stability among resource efficacy and reliability. Routing Efficiency Module provides a comprehensive method to enlightening routing performance in opportunistic networks through the use of five key enabling tools, namely: Stability Estimation, Link Capacity, Buffer Utilization, Energy Awareness and Secure Cooperation.

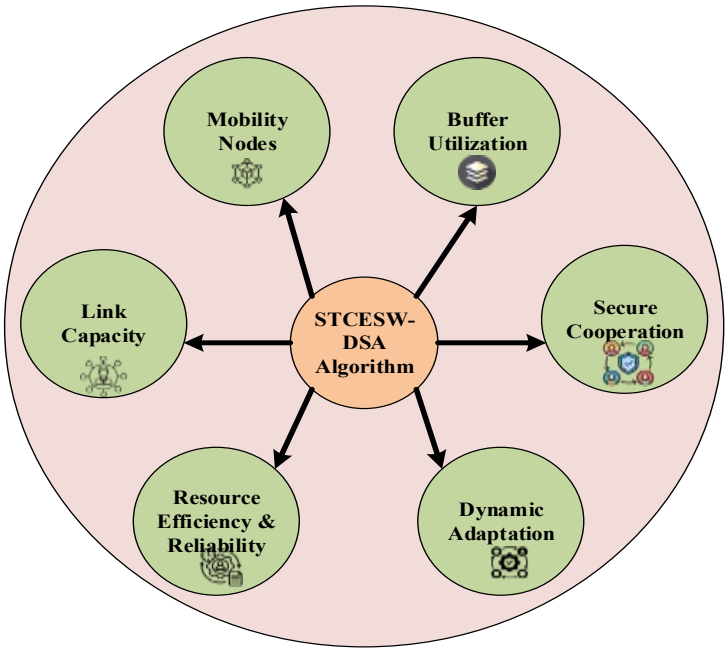

Fig 3. 1 Routing Efficiency Module

The Routing Efficiency Module creates a framework for intelligent message forwarding within an opportunistic Network (ON). The structure of the REM allows for decentralized operation, and gives each node the ability to analyze its own possibilities for forwarding messages based on real time conditions in the Network and the information that is present at each node. The first step of the REM is referred to as Node Encounter Detection, when one Node recognizes (detects) another Node within its vicinity during an opportunistic encounter. After an encounter has been recognized, the REM will call upon the Stability Evaluator Unit to calculate the Stability Score for both Nodes that were encountered.

Stability Scores are computed based on a number of important indicators which include, but are not limited to, the Mobility Behavior of a Node, Generator of Average Duration of Contact, Residual Energy of a Node, and Size of Buffer of a Node. Nodes with relatively high stability scores are considered to be the best candidates for relaying messages. At the same time, the Transmission Capacity Evaluation component determines whether the duration of the encounter will be sufficient for the successful transmission of the message payload. By only making forwarding decisions when there is sufficient time for a link to be used for the entire transmission of a message, the amount of partial transmission and lost packets due to short connection durations can be minimized.

The Dynamic Spray Adaptation (DSA) module makes real-time decisions on how many copies of a message should be sent to multiple recipients. Depending on how stable and dense the network is (and how many resources there are) the DSA will create additional copies in areas where there are fewer resources and less stability and limit the amount of copies made in areas that are stable and dense. This allows for less overhead as it minimizes the number of copies that must be sent out while still providing high delivery probabilities. The Resource Awareness aspect of the REM contains the Resource Aware Forwarding and Resource Aware Buffering functions. A Node with little remaining Energy or very little Buffer Space will not be selected as a Relay Node because it has a higher risk of dropping packets before getting to their final destination and causing Buffer Overload. Resource utilization is distributed more evenly across the network. The Trust Evaluation Module of the REM helps improve both the Security and Cooperation of the Network. Nodes are evaluated based on their ability to

Forward Messages and cooperate with other Nodes. Based on this information, a Trust Score is assigned to the Node and updated based on each successful Forwarding and Cooperative Relationship. The Routing Process will gradually isolate Nodes that continue to misspeak as Selfish or Malicious to improve the Reliability of the Network and increase Resilience to Attack.

Finally, The Forwarding Decision Engine utilizes the five inputs of Stability, Transmission Capacity, Dynamic Adaptation, Resource Awareness (Included Energy and Buffering Awareness), and Trust Evaluation to select the best Relay Node for forwarding the message using Store-Carry-Forward until it arrives at its destination Node. The Routing Efficiency Module integrates Stability Awareness, Adaptive Replication, Resource Efficiency, and Secure Cooperation into a single module that combines the benefits of each of these individual modules to provide superior routing capabilities in dynamic opportunistic networks. By reducing routing overhead, increasing delivery ratios, and decreasing the total latency of routing messages, the Routing Efficiency Module significantly improves the effectiveness of routing in dynamic and opportunistic networks. The routing efficiency can be expressed as,

$$\hat{\lambda}_{ij}(t) = \alpha\, \hat{\lambda}_{ij}(t - \Delta t) + (1 - \alpha)\, 1\{i \leftrightarrow j\ during\ [t - \Delta t, t]\} \qquad (3.1)$$

The encounter rate $\hat{\lambda}_{ij}(t)$ between nodes and is estimated using an exponential moving average (EMA), where $\alpha \in (0,1)$ represents the weighting factor controlling the influence of past contacts. The term $1\{1 \leftrightarrow j\}$ is an indicator function. This adaptive process lets contact frequency and network density vary over time.

$$\bar{\tau}_{ij} = \frac{1}{N_{ij}} \sum_{n=1}^{N_{ij}} \tau_{ij}^{(n)} \qquad (3.2)$$

The average contact duration $\bar{\tau}_{ij}$ between nodes and derived from N_i previous encounters, where $\tau_{ij}^{(n)}$ denotes the duration of the n^{th} contact. From equation 6, the node

mobility stability factor μ_i quantifies the relative stability of node i. A more stable node with less mobility that can contribute to routing stability is represented by a larger $\mu_i$value.

$$C_{ij} = \frac{B_{ij}}{T_{ij}+\epsilon} \quad (3.3)$$

The instantaneous transmission capacity C_{ij} between nodes and it is attained as the ratio of available bandwidth B_{ij}.A small constant ϵ avoids numerical instability.

$$\beta_i = \frac{b_i^{avail}}{b_i^{max}} \quad (3.4)$$

Buffer utilization ratio β_i expresses the fraction of available buffer space in node. b_i^{avail} and b_i^{max} represent available and maximum buffer sizes respectively. This term confirms that the nodes with sufficient buffer resources for message forwarding and storage.

$$\rho_i = \frac{E_i^{rem}}{E_i^{cap}} \quad (3.5)$$

The residual energy ratio ρ_i reflects remaining energy node,where E_i^{rem} denotes remaining energy node. E_i^{cap} Represents total energy capacity. Maintaining high ρ_i prevents routing decisions that could rapidly deplete node energy, supporting network longevity.

$$S_i = w_\lambda \tilde{\lambda}_i + w_\tau \tilde{\tau}_i + w_\mu \mu_i \quad (3.6)$$

The stability score S_i integrates normalized parameters of encounter frequency $\tilde{\lambda}_i$ average contact duration $\tilde{\tau}_i$ and mobility stabilityμ_i. For routing selection, this composite factor offers a single indicator of node reliability.

$$U_{ij}^{(m)} = \phi_1 R_{ij} + \phi_2 \frac{C_{ij}}{C_{max}} + \phi_3 \beta_j + \phi_4 \rho_j - \phi_5 ESS_j \quad (3.7)$$

The forwarding utility $U_{ij}^{(m)}$ of node and determining the combining link reliability R_{ij}, normalized capacity ratio $\frac{C_{ij}}{C_{max}}$, buffer availability β_j, energy ratio ρ_j, and the selfishness score ESS_j. The coefficients $\phi_1 - \phi_5$define the relative importance of each parameter ensuring balanced routing between performance , resource usage and cooperation.

$$P_{ij}^{(m)} = \frac{\exp(\gamma U_{ij}^{(m)})}{\sum_{k \in \mathcal{N}_i} \exp(\gamma U_{ik}^{(m)}) + \delta} \quad (3.8)$$

The selection probability $P_{ij}^{(m)}$ for forwarding message m is obtained using a normalized exponential function over all neighbors N_i, Where $\gamma > 0$ controls the selection sensitivity and δ prevents division by zero.

$$\Phi_{ij}^{(m)} = w_1 log\,(1 + \Pi_{i \to d}^{(t)}) - w_2 E_{i \to j}(m) - w_3 Cost_{sec}(j) \quad (3.9)$$

The final routing decision metric $\Phi_{ij}^{(m)}$ which integrates the delivery probability$\Pi_{i\to d}^{(t)}$, energy cost $E_{i\to j}(m)$, and security $Cost_{sec}(j)$ .The logarithmic term is used to enhance the stability against large probability variations. The node maximizing $\Phi_{ij}^{(m)}$ is selected as the optimal forwarder, ensuring an efficient and secure data delivery process. Pseudocode for routing protocol efficiency is presented in Algorithm 1.

3.2 Algorithm (with Time and Space Complexities)

Algorithm 1: Routing protocol efficiency

Data: Node encounter records$\{\lambda, D\}$, mobility status $\{v\}$,

buffer usage $\{B\}$, residual energy $\{E\}$

Input: Stability weights $(\beta_1, \beta_2, \beta_3)$, utility weights

$(\delta_1, \delta_2, \delta_3)$, copy control factor k

Result: Efficient and stable next hop selection for message

forwarding

1. Initialize stability parameters for all nodes

2. Compute initial encounter rate λ_{i_j} and contact duration D_{ij}

3. Compute node stability S_i using λ_{i_j} and contact

duration D_{i_j}

4. While message is active do

5. Update S_i and link capacity C_{i_j} for current neighbors

6. Evaluate buffer ratio B_j and energy ratio E_j

7. Compute forwarding utility U_{i_j} for each neighbor j

8. Select next hop $j^* = argmax(U_{ij})$

9. Adapt message to $j*$ only if resource constraints are satisfied

10. Forward message to $j*$ only if resource constraints are satisfied.

11. Suppress redundant transmissions by ignoring low utility nodes

12. End while

13. Return Optimal Forwarding decision and updated stability metrics

---

Time Complexity Analysis

1. Computing stability for N nodes $\rightarrow O(N)$

2. Evaluating forwarding utility for k neighbors $\rightarrow O(k)$

3. Making forwarding decisions for m messages $\rightarrow O(mk)$

$$T_{STCESW-DS} = O(N + mk)$$

Space Complexity Analysis

1. Storing stability metrics for N nodes → $O\ (N)$

2. Storing neighbor-specific parameters (buffer, energy,

utility) → $O(k)$

$$S_{SECESW-DSA} = O(N + K)$$

An algorithm is proposed in this paper to improve the routing efficiency in an opportunistic network through smart selection of the most stable and resource-aware next hop for message forwarding. The new algorithm uses a combination of evaluating node stability, assessing resource availability, and computing the adaptive forwarding utility of a node to assist in making intelligent routing choices in a very dynamic network environment.

At the beginning of the process, the algorithm has gathered all node encounter information. This includes both the encounter rate (λ) and the length of time of contact (D) that occurred, together with the mobility status, amount of buffer space used, and residual energy of each node. In addition, stability and utility weights will be established as input variables in order to balance how much the social interaction patterns will affect routing decisions relative to the resource constraints. Also created is a copy control factor to manage the amount of message replication and to keep message flooding to a minimum.

During the initialization step, stability parameters will have been assigned to all nodes based on past encounter data. The first encounter rate and contact length calculations between nodes will have taken place, which will act as the primary indicators of how stable the node remains. Based on the calculated encounter rate and the contact length, stability scores will be assigned to each node based on each node's probability of establishing reliable communication links over time. The algorithm updates both the stability score and link

capacity of neighboring nodes on the network after every recent encounter when a message is still "alive" in the network. During this phase, it also looks at both the available buffer space and the remaining energy of each neighbor to make sure it doesn't overload its resource-poor neighbors with the forwarding decision. To determine how much utility each neighbor has for forwarding, a forwarding utility function for each neighboring node is calculated by combining its stability score, buffer space ratio, and energy ratio. Pre-defined utility weights are used in this calculation.

The neighbor that provides the most value (the highest utility) will be selected as the next hop to forward the message. However, forwarding messages can only occur if the selected neighbor meets specific resource requirements such as available buffer space and sufficient energy. In addition, since redundant transmissions should be avoided, neighbors with low utility values will be excluded from further consideration, reducing the number of duplicate messages sent and thus reducing the amount of routing overhead required to send those messages.

After the selection of the optimal next hop has been completed using the above method, stability metrics will be returned for that neighbor so that stability metrics can be used in making subsequent routing decisions. Thus, the routing protocol will be able to adapt to frequent topology changes while ensuring reliable delivery of messages.

The STCESW-DSA network routing algorithm has three primary components that can be expressed as a function of time complexity:

- The computation of stability metrics for every node in the network (N nodes) has an $O(N)$ time complexity.
- The computation of the forwarding utility associated with the k nearest neighbours of the node being evaluated has a $O(k)$ time complexity.
- After forwarding decisions have been made for m number of messages, the total complexity associated with computing the forwarding decision becomes$O(m * k)$.

Therefore, using the above factors, the overall time complexity of STCESW-DSA is given as follows:

$$T_{STCESW-DS} = O(N + mk)$$

The space complexity of the algorithm is based on the storage of stability metrics for nodes and neighbour-specific parameters which will have an impact on the space used.

In addition to requiring $O(N)$ of space to maintain stability information for each of the N nodes, the same is true for the k neighbours - To maintain the status of buffers, energy levels and utility values requires $O(k)$ of space.

Therefore, the overall space complexity will be:

$$S_{SECESW-DSA} = O(N + K)$$

The proposed routing protocol is efficient in its use of memory and can be utilized in the deployment of opportunistic networks of large scale.

3.3 Experiment Setup (with ONE Simulator)

3.3.1 Simulation Setup

The section shows set up for ONE simulator. To simulate the proposed research method, Java language version JDK 21.0.5 is used [208]. The Table 3.1 displays ONE Simulation Parameters

Table3. 1 One Simulation parameters

Category	Parameter	Value(s)
Scenario	Data Propagation	STCESW-DSA (Proposed Approach)
	Update Interval	0.1 s
	SimulationTime	43200 s (12 h)
Interfaces	Interface	Bluetooth
	btInterface Type	SimpleBroadcastInterface
	btInterface Speed	250 kbps
	Group Buffer Size	Group Buffer Size 5 MB (default), 50 MB (trams)
	Group Speed	0.8–2.5 m/s (pedestrians), 2.7–13.9 m/s (cars), 7–10 m/s (trams)
Mobility	Movement Model	Shortest Path Map Based Movement, Map Route Movement (trams)
	World Size	4500 × 3400 m
	Map Files	roads.wkt, main_roads.wkt, pedestrian_paths.wkt, shops.wkt
	Interval	10–18 s
	Message Size	500 KB – 1 MB
	Hosts	0–99

	TTL	20000 s

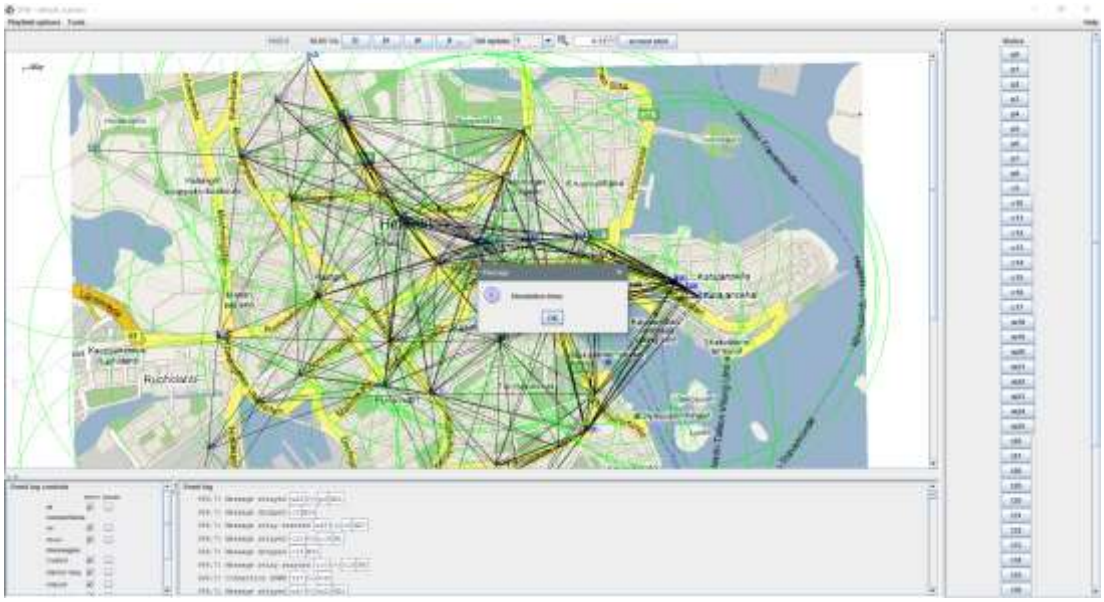

Fig 3. 2 ONE Simulation Network

3.3.2 Comparative Analysis

For comparison, the ECSUO ("Edge community service in opportunistic social networks") model is refereed as it is presently the leading existing approach for routing in opportunistic network. ECSUO provides community-based forwarding but suffers from higher overhead ratio under dynamic conditions, making it suitable to evaluate improvements in the proposed STCESW-DSA routing model. The proposed method is evaluated by comparing with the existing method in following domains: Time Vs delivery ratio and Time Vs Overhead ratio. Compared to the existing method, ECSUO, the proposed STCESW-DSA method gives good performance. In Fig. 3. 2, the ONE simulation network environment is configured with realistic contact patterns, node mobility and wireless communication properties to closely represent real-world dynamic network conditions and the opportunist network is constructed with 100 nodes.

3.3.2.1 Number of Nodes Vs Delivery ratio (%)

The number of nodes in a network because more contact points creates more possible forwarding paths. In high node density opportunistic nets where our new routing algorithm (STCESW-DSA) will operate, the routing algorithm will take advantage of the node's stability, as well as its probability of being encountered, to select the best possible relayers for sending messages. STCESW-DSA's Routing Efficiency Module (REM) limits the number of times a message needs to be replicated and routes messages only via stable and well-resourced nodes, unlike previous routing methods used for sending messages across opportunistic networks through simple flooding of messages. As demonstrated by the delivery ratio remaining high, we have a routing strategy that is robust to changes in density.

Table3. 2 Number of Nodes Vs Delivery ratio (%)

Number Of Nodes	Delivery ratio (%)	
	STCESW-DSA (Proposed)	ECSUO (Existing)
50	50	55
100	58	60
150	65	65
200	66	70
250	68	75
300	78	80
350	85	85
400	95	90

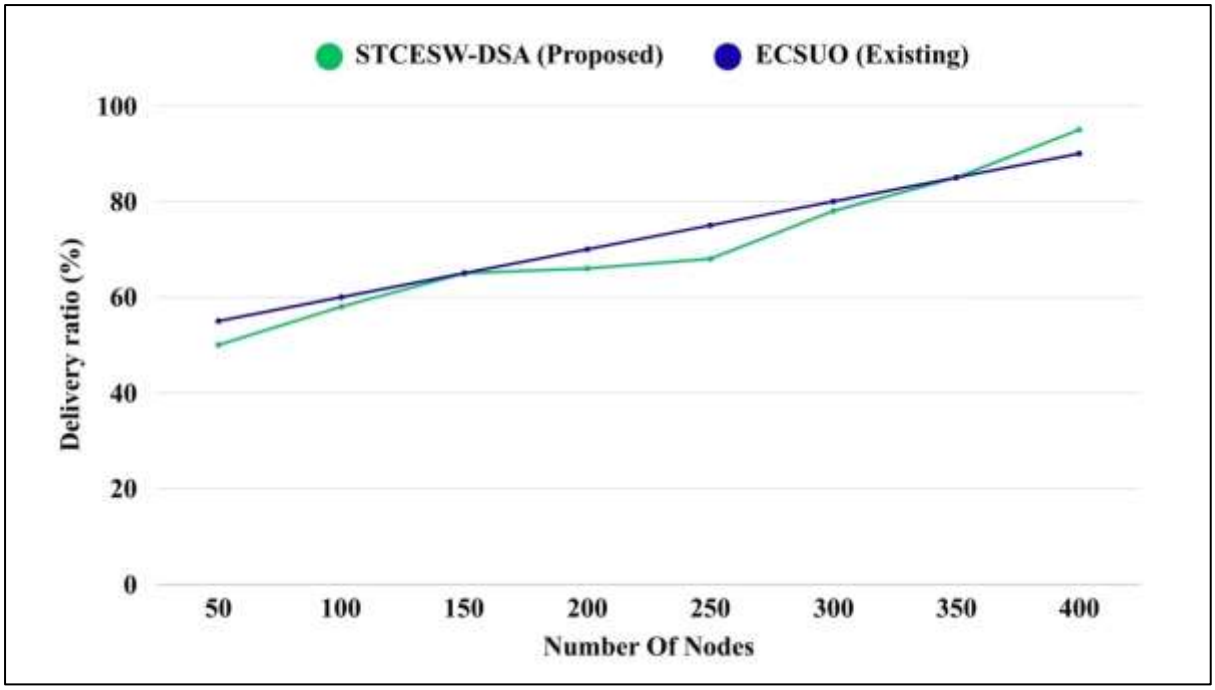

Fig 3. 3 Number Of Nodes Vs Delivery Ratio (%)

In table 3.2 and Fig 3.3 Depict how many successful transmissions there were from the first source node to the last sink node as the number of nodes in the routing protocol increases. With both the STCESW protocol and the ECSUO routing protocols, the number of successful transmissions improved as the density of the node increased from 50 nodes to 400 nodes. The increased density of the node allowed for more contact with more nodes, thereby allowing for greater opportunities for nodes to be connected to each other. When there were low densities of nodes (50-100 nodes), the ECSUO routing protocol performed about 5%-6% better than the STCESW protocol on average. The reason for this is because of the limited number of encounters that existed which reduced the effectiveness of the stability aware efforts that were included with the STCESW protocol, while at medium densities of nodes (150-250 nodes), both protocols had very similar performance (with the STCESW protocol continuing to show a steady increase). When there were high densities of nodes (300-400 nodes), the STCESW protocol had a success ratio of about 95% while the ECSUO protocol had a success ratio of about 90% which amounts to approximately a 5.6% increase in success rate for the STCESW protocol. These results demonstrate how the stability aware spray and wait approach that was developed provides an effective means for reducing redundant

transmissions which results in increased reliability in delivering messages in high-density opportunistic network environments.

3.3.2.2 Number of Nodes Vs Average Latency(s)

The average amount of time that it takes for a message to travel from the source to the destination is referred to as average latency. Increasing the number of nodes increases the average latency because of buffering delays, forwarding contention, and hop counts among the nodes. By prioritising nodes that have longer chances of being encountered and have predictable mobility patterns, the routing algorithm will reduce average latency and increase the speed at which messages can be propagated from the source to the destination. The dynamic copy-control mechanism in the routing algorithm will also reduce average latency by limiting message congestion created by excessive duplication of messages and increased latency. The result is that average latency is lower than average latencies produced by previously used opportunistic routing protocols, thus demonstrating efficient use of contact opportunities and timely delivery of messages.

Table3. 3 Number of Nodes Vs Average Latency(s)

Number Of Nodes	**Average Latency(s)**	
	STCESW-DSA (Proposed)	**ECSUO (Existing)**
50	5	7
100	8	10
150	12	15
200	15	17
250	16	18
300	17	19
350	20	21
400	31	33

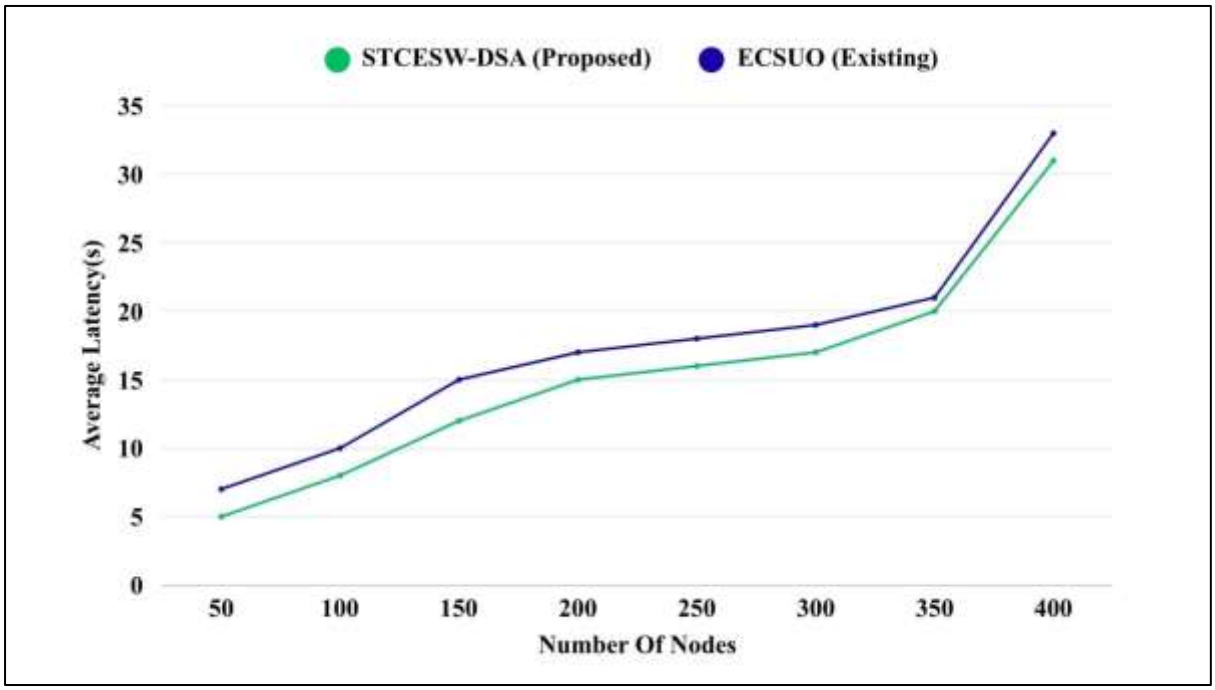

Fig 3. 4 Number Of Nodes Vs Average Latency(s)

In table 3.3 and Fig 3.4 Average latency as a function of the number of nodes, with both proposed STCESW-DSA routing approaches and existing ECSUO routing schemes shown in Fig. X, show similar performance. Latencies for both approaches will continue to increase as the number of nodes increases due to the increased number of users vying for the same wireless link, thus increased levels of contention, increased buffer usages and added amount of time spent waiting for packets to forward are all related to an increase in the total number of nodes used in opportunistic networks (as a general rule, lower node counts have less delay due to the lower overall traffic on the network). When node densities are low (50 nodes), STCESW-DSA's total latency is approximately (5 seconds longer) lower than ECSUO's (7 seconds); therefore, STCESW-DSA achieves a 28.6% lower overall latency than ECSUO. At moderate densities (100 to 200 nodes), there is little to no difference in total latencies as both approaches exhibit the same level of performance with regard to forwarding packets due to similar numbers of contact opportunities that were available to each protocol. At a node count of 250, STCESW-DSA decreases the overall latency as it goes from 25 seconds to 23

seconds, or an approximate reduction of 8% from the average latency observed using the ECSUO routing scheme (ECSUO's average latency was 30 seconds). When node counts increase to 300 to 350 nodes, both protocols operate at the same level of performance; however, when increasing node count to 400 nodes, STCESW-DSA's performance is reduced by 0.4 seconds. Overall, it can be said that STCESW-DSA minimizes the impact of delays caused by the distance from the source end to the destination end for both very sparse and moderate density networks while maintaining a significant amount of delay via similar performance levels in larger scale environments.

3.3.2.3 Number of Nodes Vs Overhead Ratio (%)

By measuring the redundancy in message transmission, the overhead ratio is an indication of how effectively the routing protocol is configured and working. Uncontrolled replication in a dense network can create an excessive amount of overhead, so adaptive forwarding/selective replication as used by STCESW-DSA provides a significant decrease in redundant transmissions through its use of Node Stability Metrics (NSM). The slight increase in the amount of overhead as the number of nodes in the network increases indicates that the scalability of this protocol is efficient. The lower level of overhead also indicates an improvement in the efficient use of network resources and signifies that there are optimal routing decisions in place within the context of a large-scale deployment of opportunistic networks.

Table3. 4 Number of Nodes Vs Overhead Ratio (%)

Number Of Nodes	Overhead Ratio (%)	
	STCESW-DSA (Proposed)	ECSUO (Existing)
50	7.0	9.0
100	6.8	8.8
150	6.5	8.5

200	6.0	8.3
250	5.5	8.2
300	5.3	8.1
350	5.2	8.0
400	4.0	7.5

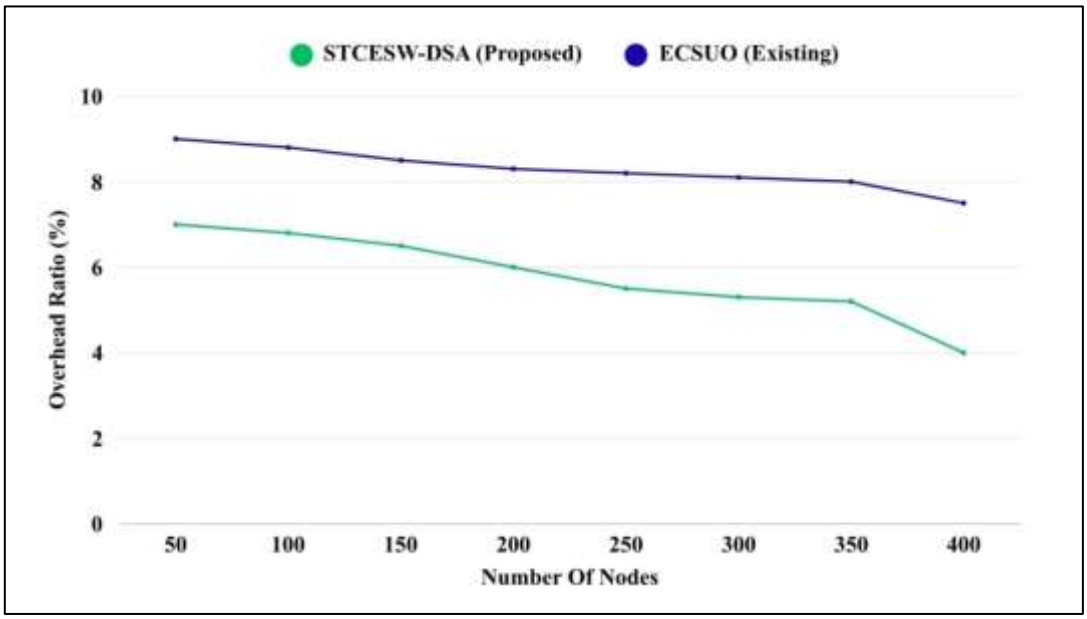

Fig 3. 5Number Of Nodes Vs Overhead Ratio(%)

In table 3.4 and Fig 3.5 Graph above illustrates the difference in routing overhead as the network grows larger using STCESW-DSA compared to using ECSUO. The ratio of Routing Overhead for each protocol decreases as Net Node density increases. However, STCESW-DSA continues to have Lower Routing Overhead vs the other protocol in all node counts. For example, with 50 Nodes STCESW-DSA has 7% routing overhead while ECSUO has 9%. When the number of nodes becomes 400, STCESW-DSA reduces Routing Overhead to 4% whereas ECSUO keeps 7.5%. The decrease in Routing Overhead supports the benefits of a Stability Aware Forwarding Strategy, avoiding redundant message replication and reducing redundant message transmission.

3.3.2.4 Number of Nodes Vs Average Buffer Time(s)

"AvgBufferTime" refers to the average amount of time that messages spend in the buffer of a node before they are forwarded/delivered. As networks become larger, more inefficient means of managing buffers will result in higher instances of packet drops and network congestion. The current proposal solves this problem by selecting relay nodes that have enough available room/buffer and have stable contact behaviours. By reducing the number of unnecessary copies of each message and focusing on sending messages via the most efficient means possible, the amount of time that a message spends in the buffer is also reduced. This will reduce the amount of congestion in the network, increase throughput, and help to stabilize the network.

Table3. 5 Number of Nodes Vs Average Buffer Time(s)

Number Of Nodes	Average Buffer Time(s)	
	STCESW-DSA (Proposed)	ECSUO (Existing)
50	18.0	21.0
100	17.8	19.8
150	15.5	17.5
200	12.3	15.3
250	10.0	14.2
300	9.3	12.1
350	7.5	8.0
400	6.0	6.0

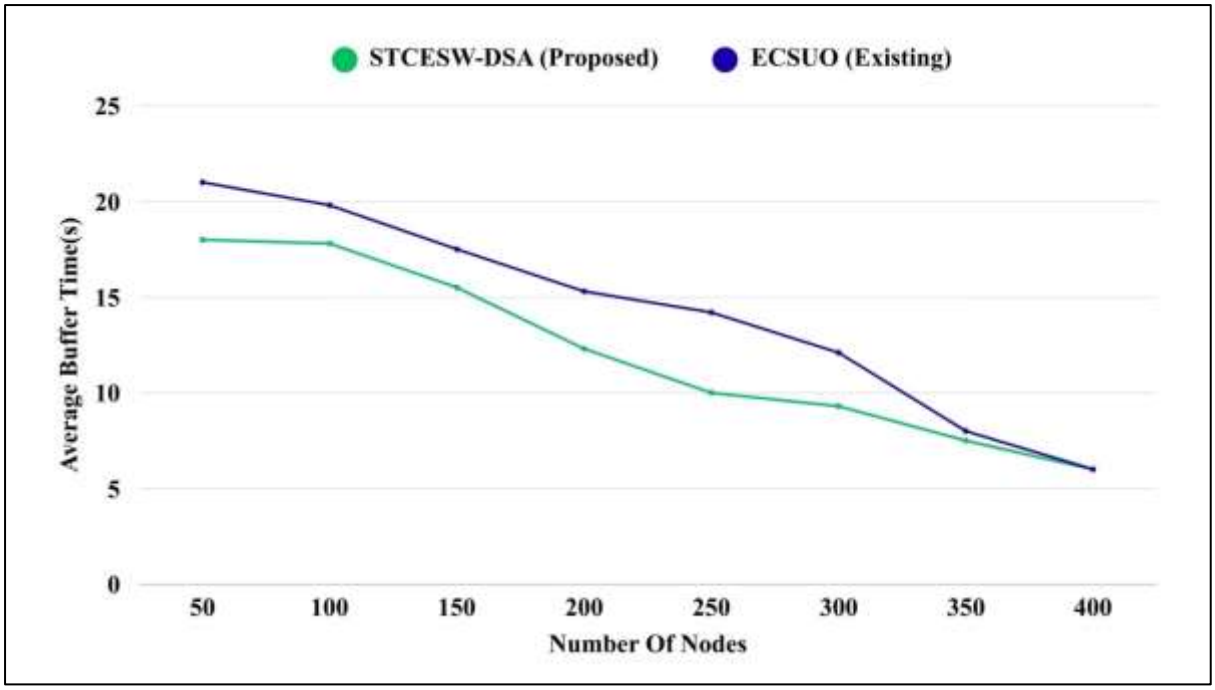

Fig 3. 6 Number Of Nodes Vs Average Buffer Time(s)

In table 3.5 and Fig 3.6 This graph shows how long it takes your packets to be sent to their destination when they arrive at your buffer (or memory location) from the network. By demonstrating that STCESW-DSA has less time spent in buffering than ECSUO, you can see the difference in numbers at the 50 node mark for STCESW-DSA has 18 seconds and for ECSUO 21 seconds. As the node density increases, the time spent storing packets in buffers decreases for both protocols because both protocols have better opportunities for the packets to connect. When you get to 400 nodes the two protocols will have approximately the same amount of time (6 seconds), which means that dense networks of nodes can utilize their buffers more efficiently. The fact that STCESW-DSA shows less buffer time relative to other protocols demonstrates that it has better scheduling and more managed packet duplication.

3.3.2.5 Number of Nodes Vs Energy Consumption (J)

In opportunistic networks, where nodes function under resource constraints, energy consumption is a major factor. Typically, energy consumption grows with the increase in node count due to the increased frequency of both transmitting and receiving messages. The STCESW-DSA Routing Protocol limits energy consumption through the elimination of

redundant message forwarding and by selecting energy-aware stable nodes as relay nodes. As a result, by minimizing processing time and transmission time, this approach conserves energy on each individual node. In fact, the results suggest that this approach to routing will be effective for opportunistic networks that are both large-scale and operate in an energy-constrained manner.

Table3. 6 Number of Nodes Vs Energy Consumption (J)

Number Of Nodes	Energy Consumption (J)	
	STCESW-DSA (Proposed)	ECSUO (Existing)
50	2	5
100	5	15
150	10	25
200	12	35
250	15	45
300	20	55
350	25	75
400	26	95

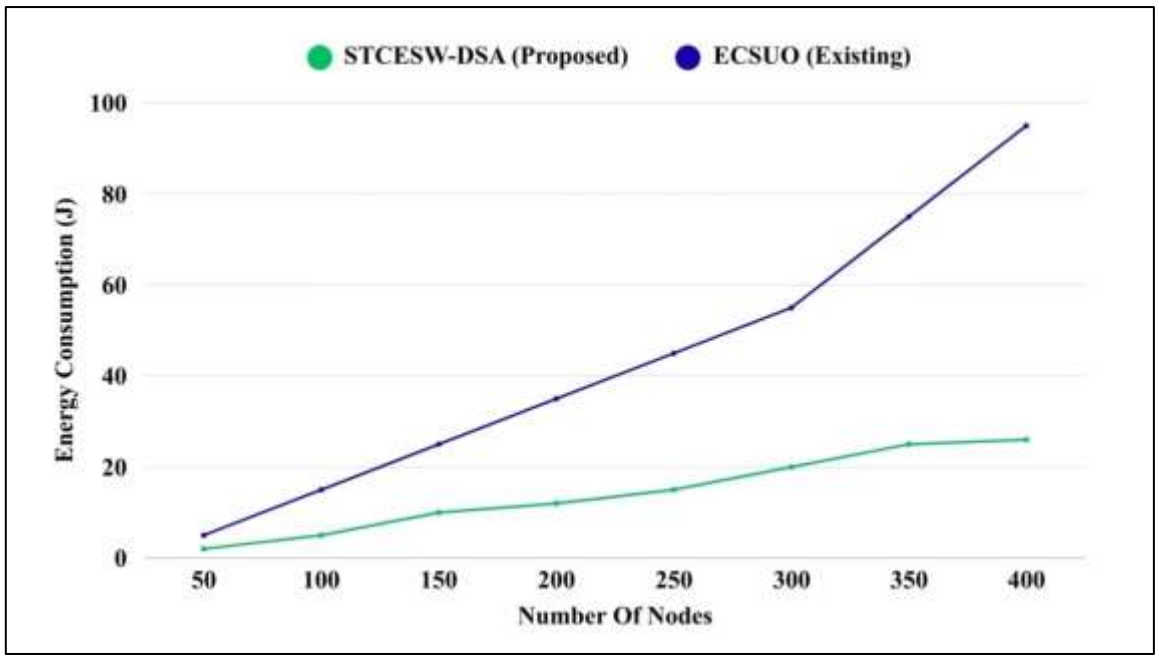

Fig 3. 7 Number Of Nodes Vs Energy Consumption (J)

In table 3.6 and Fig 3.7 this diagram represents the routing protocols with an emphasis on their energy efficiency. As the number of nodes increases, so too does the amount of energy consumed per node due to the increasing number of forwarding and control messages. Furthermore, STCESW-DSA has much less energy consumption than ECSUO, with STCESW-DSA using 2 J of energy at 50 nodes and 5 J of energy from ECSUO at that same point. STCESW-DSA also saves energy through more controlled thoughtful decisions related to how an overall spray occurs. At the 400-node comparison, STCESW-DSA consumes 26 J as opposed to 95 J from ECSUO demonstrating a marked energy savings due to this routing technique.

3.4 Results and Discussion

The research utilizes the ONE simulator to conduct a large-scale Opportunistic network (OppNet) consisting of100 mobile nodes. The simulation environment defines realistic node mobility patterns, contact behaviours, and wireless communication characteristics to closely resemble real-world opportunistic networking scenarios. Using this configuration, the network is modeled and simulated to evaluate the routing performance of the proposed STCESW-DSA routing model under dynamic and intermittently connected conditions.

The simulated network performance is analyzed using key performance metrics such as packet Transport Time, Packet Size, and Packet Count on Receipt. Additionally, the routing efficiently of the STCESW-DSA model is evaluated through comparative plots of Time versus Delivery Ratio and time versus overhead ratio. These metrics provide insight into the effectiveness of the routing strategy in terms of successful message delivery and resource utilization over varying simulation durations.

Simulation results indicate that the STCESW-DSA routing model achieves a consistent improvement in delivery performance across all simulation time periods. As simulation time increases, a gradual and sustained rise in delivery ratio is observed. This trend demonstrates that the gradual and sustained rise in delivery ration is observed. This trend demonstrates that the routing model effectively exploits increasing contact opportunities over time and adaptively selects forwarding nodes based on evolving network conditions. The ability to leverage accumulated contact history allows the routing mechanism to make more informed relay decision, thereby improving message delivery success.

In the Time Versus Delivery Ratio analysis, STCESW-DSA consistently outperforms the comparison routing protocols throughput the entire simulation duration. During the initial stages of the simulation, delivery ratios remain relatively low due to limited node encounters and insufficient contact history. However, as time progresses and knowledge of node stability and link duration, resulting in a significantly faster increase in delivery ratios compared to traditional opportunistic routing approaches that rely primarily on probabilistic or forwarding mechanism.

The feature of message forwarding in STCESW-DSA facilitates maximum adaptability under different scenarios of node mobility, contact, and resource availability. With the emphasis on stable nodes with higher predicted contact periods, this approach minimizes unnecessary message drops involving short-lived node connections, buffer overflows, and excessive replication. This facility is most useful at medium to high node densities, where replication results in performance deterioration.

The Time vs. Overhead Ratio analysis serves to confirm the efficiency of the proposed STCESW-DSA model. The implementation of a resource-aware copy control within the routing framework has enabled it to significantly reduce congestion within the system while at the same time facilitating efficient message transmission through a controlled replication mechanism, whereby a limited number of message copies are produced, unlike conventional routing protocols.

Overall, the experimental results clearly confirm that the proposed STCESW-DSA routing model achieves an optimum trade-off between high delivery performance and low routing overhead in opportunistic network environments. The stability-aware, dynamically adaptive forwarding strategy of the proposed routing model enhances the robustness and scalability of OppNets in dynamic mobility and intermittent connectivity conditions; hence, this scheme is suitable for large-scale deployment of OppNets.

3.5 Summary

The Research presents a new method concerning a Routing Efficiency Module (REM) as proposed in the STCESW-DSA routing algorithm solution to these important problems faced by Opportunistic Networks such as High routing overhead, message flooding, and unstable message delivery as well as to better understand the concept of Node Stability through Evaluations based on various Types of Parameters representing a node's current state - including, but not limited to: mobility behaviour, encounter rate/contact duration/residual energy/buffer availability - thus enabling the appropriate decision-making process when attempting to Forward Messages intelligently and adaptively in what is an Extremely Dynamic & Rapidly Changing Network Environment is equal to STCESWDSA. A Method for Dynamically Controlling the Number of Copies of a Message Replicated in Time and Place and/or for Selecting a Stable Relay Node for holding on to duplicate Messages, thereby Minimising Unnecessarily Transmitting Messages their associated routing overheads) yet still supports Reliable Communication thus allowing the Network to Improve Overall using a Very Adaptive Routing Protocol that is computationally efficient & scalable making them Ideal for very Large Deployments of (OppNets) The routing performance is increased by using this routing framework, allowing Messages to be sent reliably to their intended Destination while also decreasing Network Instability, increasing Sender & Receiver Node Communication-Efficiency and maintaining Node Stability. Finally, the STCESW-DSA routing algorithm shows how intelligent forwarding decisions based on live Node Stability Metrics allow for less frequent Message Replication and Network Congestion. Ongoing Node Activity and Environmental Condition Monitoring enables dynamic protocol adaptation to frequent Topology changes typically associated with Opportunistic Networks using the Routing Efficiency Module (REM).Message forwarding through nodes exhibiting stable contact patterns and adequate resources will help prevent message loss because of buffer overflow, battery depletion or intermittent connectivity. The dynamic copy control strategy featured within the proposed solution provides a critical function in reducing latency,

improving buffer management, and minimising energy usage to enable sustainable long term operations. Instead of blindly flooding the network with many copies of messages, STCESW-DSA uses the stability of nodes and the predictability of encounters to decide how many times to replicate a message.

This type of selective replication allows for reduced overhead, while still achieving a high success rate in delivering messages through medium-to-high density networks. In turn, this improvement in the performance of the communication system provides an increase in the network's lifetime through better performance in message buffer management, lower total power usage by each node during delivery and improved latency.

When Stability-Aware Relay Selection is utilized, it provides an increased probability that a message will be delivered via the node with the highest chance for success. This leads to decreased handoff/retransmission events due to the frequent occurrence of instability or inefficiency found in all traditional opportunistic routing protocols. The routing framework presented in this paper includes a mechanism for the selection of nodes with consistent mobility patterns, as well as nodes with the longest contact periods, therefore increasing both the survivability and continuity of messages on fragmented networks. The resulting Adaptive Routing Decision, Dynamic Copy Control, and Node Stability Evaluation (STCESW-DSA) Routing Solution provides a complete solution for the greatest opportunistic networking challenges The results suggest that the implemented protocol dramatically enhances both the performance and scalability of the delivery of packets across a network, offering significantly improved levels of robustness with regard to dynamic environments. Consequently, based upon the research undertaken, as well as the performance metrics evaluated, the routing methods based upon STCESW-DSA represent a feasible, efficient, and scalable solution to routing within a large scale opportunistic network implementation and environment where traditional approaches do not perform optimally due to constant disconnections or fluctuating node behaviours.

Chapter 4

The SPONS is a secure and privacy-preserving framework for opportunistic networking employing the SORSI trust and incentive model, in combination with HIBS encryption. It is designed to identify and confront selfish nodes, encourage users to cooperate, establish low-overhead secure end-to-end communication, and perform better than all previously proposed secure protocols with respect to delivery ratio, latency, overhead, buffer usage, and energy efficiency, as well as offering excellent levels of security and privacy.

Section 4.1 describes the proposed security framework and privacy framework with the SORSI and HIBS components. Section 4.2 provides information about the Identity-based Cryptography model, and the Social-based Routing approach of the proposed security framework.Section 4.3 contains the algorithm for secure communication in both time and space complexity analysis.Section 4.4 includes an explanation of the experimental setup including simulation parameters and network configurations. Section 4.5 contains results from each experiment with a comparative analysis of them demonstrating the effectiveness of SPONS. Finally, Section 4.6 summarizes the major contributions and findings of the proposed security framework.

Security and Privacy in Opportunistic Networks

Opportunistic Networks (OppNets) use human mobility as well as local forwarding methods for data distribution purposes. This can happen by either being able to store and forward data based on the user's mobility or having the ability to send data over a wireless link when an appropriate contact is made with another device. OppNets exist at the intersection of Mobile Ad-Hoc Networks and Delay-Tolerant Networks. What differentiates them from the others is that OppNets utilize the opportunistic sending of messages; they do not have end-to-end communication paths for data transfer [116]. The fundamental building block that underlies the work of OppNets is the carry-and-forward method; messages are stored in buffers located in each of the intermediate nodes until they are eventually delivered to their intended recipients. The SORSI Algorithm ("Social-based Opportunistic Routing with Selfishness Detection and Incentive Mechanism") identifies selfish nodes in opportunistic networks (OppNets) by the "Encounter-based selfishness score (ESS) mechanism." The ESS scores are assigned to all nodes in the OppNet based on their forward messages; as a result, each node's ESS score will change depending on how many messages it forwards. If a node has an Increased ESS score compared to other nodes, the SORSI Algorithm considers this node "selfish" and does not allow any other nodes to forward any messages to this node[210-212]. If a node has a decreased ESS score, the incentive mechanism rewards this node for its actions. The first is security and privacy are created using a Hierarchical Identity-Based Security Method (HIBS). This method creates a unique identifier for each node within the OppNet, allowing each node to encrypt messages using only the destination node identifier and, therefore, not requiring the use of a Certification Authority (CA) to establish secure communication between nodes. Finally, the HIBS method will ensure that only the destination node can decrypt the message from the source node and that no intermediate nodes can decrypt the message while forwarding it. A hierarchical framework for 6G-enabled IoV's attack detection is outlined in this paper.

The detection framework will utilize the edge nodes, which are designed to meet the primary 6G Key Performance Indicators (KPI) of trustworthiness, latency, connectivity, data rate, and energy usage. Attack model training and detection improvements with FL and non-cooperative gaming techniques will ensure continual improvement of the attack detection and classification processes. The cooperative method for attack detection using FL is performed by the security entities, IoV devices, edge servers, and Security Information and Event Management (SIEM) stakeholders, which ultimately results in improved accuracy rates in future attack detection classes. To strengthen the security of the proposed framework for attack detection, the authors create a competitive Stackelberg security game that helps identify IoV devices/servers that have been compromised by adversaries and provides information about the devices/servers that should be selected to participate in training, detecting, and classifying attacks against IoV and 6G networks. Most research regards Blockchain as permanent storage for secured data. Also used for purposes of Authentication. There are significant advantages to using permanent Blockchain storage due to its ability to maintain the integrity of data, along with increased efficiency for the Authentication process. Integrity and Distribution of Data provides Security for both Data Transmission and Data Storage. Blockchain's encryption is expected to provide a secure method of future operations that will address the current security issues present in other electronic health monitoring systems [213-214]. Basically, these systems use various types of encryption to encrypt data, thus preventing someone who is not authorized from easily accessing that data. A new model for securing Wireless Sensor Networks has been developed in this study that considers application requirements, the level of security, and the bit-error rates (BERs). In this case, the frame-control field (FCF) of the Zigbee MAC header was also used as an option for users to select between secure/insecure modes by utilizing the reserved bits. Self-play has previously been demonstrated to work very well in a number of different areas, and it appears that the same is true for network security in that self-play can also be effective for developing secure measures for networks. The convergence of the policies shows that the final policies are a reflection of the common-sense knowledge that humans possess, and the emergent policies closely resemble the types of strategies that are used by humans. As the open Wireless

Medium presents a unique set of challenges related to transmission uncertainty, we need to employ Interval Type 2 Fuzzy Logic Controllers as an approach for evaluating trust associated with transmission. Acquired using either the Static Deployment Method (SDM) or the Dynamic Deployment Method (DDM), sensors are used to read various data types and communicate those findings back to the users. WSIoT faces unique hurdles, which include limited memory, absence of space (voids), a high number of possible communication paths, weak security measures, and slow transfer speeds. The current research presents a Decentralised E-Government framework comprised of integrated Threat Detection features to meet the above-mentioned challenges. The encryption, validation, and immutability of Blockchain ensure that the eGovernment system maintains its Privacy/Security. Consequently, this article presents a secure Blockchain-based model that provides reliable authentication of nodes and assurance of integrity of Data while providing secure Data transmissions within a fog computing environment. For more than years of intensive research and many advances in digital, a major application area for these technologies has been security and related areas. In fact, computer vision is now considered one of the leading areas of innovation within the computer science discipline. Therefore, the effective motivation of node cooperation and the prevention of any acts of maliciousness through strict security protocols require a robust incentive structure that is put in place by the SAN. This will help to

maintain the efficiency of the SAN and to enable secure data communication within the SAN. The key challenges to securing Wireless Sensor Networks (WSNs) arise from the need for secure routing schemes, as well as the known vulnerabilities of existing routing protocols. Routing protocols, most of which emphasise computational efficiency, do not provide adequate levels of security against potential attacks, thereby rendering these protocols vulnerable to attack from malicious entities. While reactive routing protocols use the least amount of bandwidth and therefore may seem to provide the highest level of security, they also have limited network routing resources, thus presenting additional security challenges. Conversely, while the use of proactive routing protocols may provide greater levels of security, this typically requires increased resource requirements for the maintenance of network routes. Data transmitted over networks is more likely to be subject to a larger number of potential security issues. For this reason, research has been done on how best to ensure the security of data moving across networks. The goal of the author of this research article was to develop an energy-efficient and secure heuristic-based routing (SEHR) protocol for wireless sensor networks (WSN) to allow for the identification and prevention of compromised data within WSNs while maintaining a high level of performance. Our goal is to demonstrate the potential of using opportunistic authentication factors to improve IoT Security. Our position is that Sensors can serve as a means of creating new authentication factors that can complement existing Object-To-Object Authentication methods. A Framework or Foundations to Protect Data within Mobile Internet of Things Devices. Two Functions to Provide Improved Data Security with Less Energy Consumption. Opportunistic computing services are provided using the concept of self-organized ad hoc resource pools within the mobile environment. However, the dynamics and distributed nature of the mobile ad hoc network create many difficulties in terms of privacy and security within such ad hoc resource-sharing activities.

4.1 Proposed Methodology

The performance of numerous protocols associated with OppNets is subject to a variety of issues related to protocol overhead and message flooding. Consequently, a combined

mechanistic and algorithmic approach for Improved Recognition of Routing Protocols in and Improved Routing Efficiency in Opportunistic Networks is proposed in this study. This consists of the development of algorithms for improving routing and the effectiveness of communication in Opportunistic Networks. This methodological approach will be referred to as "Security and Privacy in Opportunistic Networks (SPONS)."

A. Security and Privacy in Opportunistic Networks

The “Social-based opportunistic routing with selfishness detection and incentive mechanism (SORSI) algorithm” detects the “selfish nodes” in OppNets based on the “Encounter-based selfishness score (ESS) mechanism”. Each node is assigned to the encounter-based selfishness score. And it’s based on the forwarding messages that the node score can be increased or decreased. The SORSI algorithm labels an ESS score-increased node as a selfish node. And this algorithm ensures that labelled selfish nodes don’t forward any messages to these nodes. The ESS score decreased node should be appreciated by the incentive mechanism. To enhance security and privacy in the opportunistic networks, using hierarchical identity-based security creates a public key to encrypt the message using identity based on the destination node, and without a certificate authority, it must ensure secure communication because it does not decrypt the message of the intermediate nodes while forwarding the message.Fig. 4 .1 depicts the security and privacy of opportunistic networks.

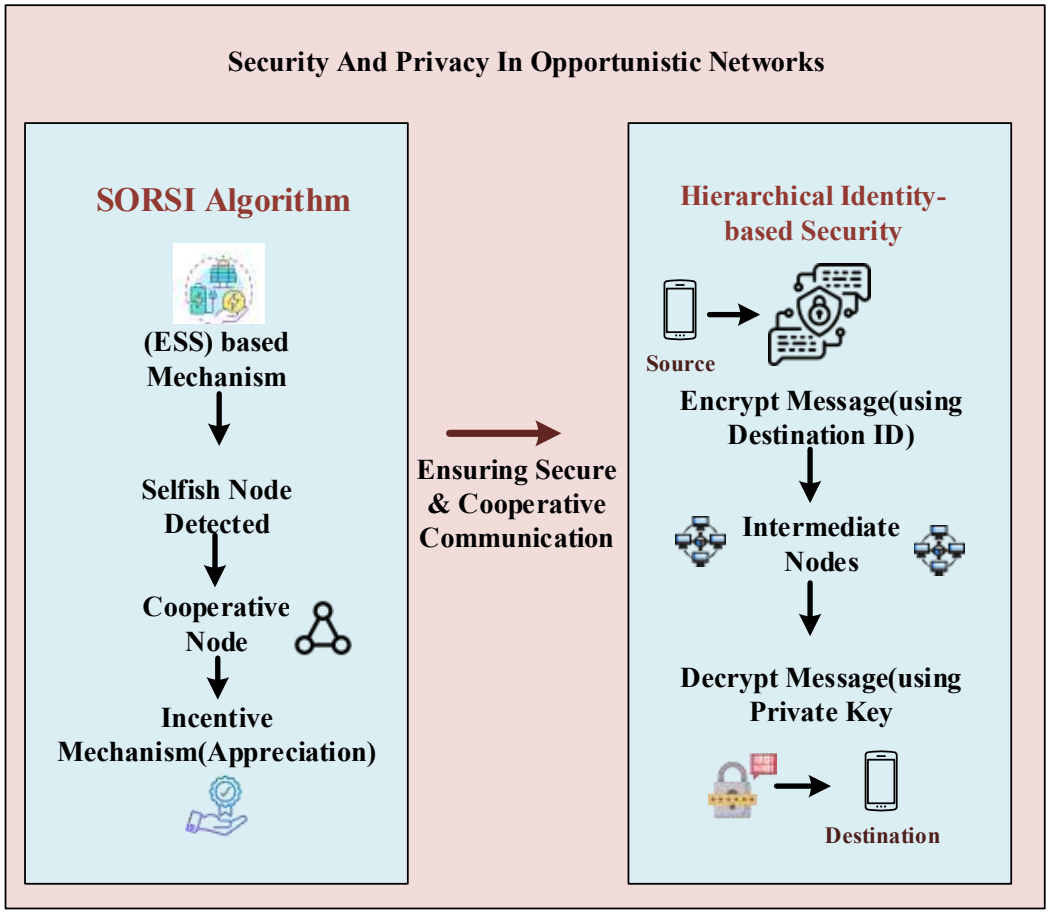

Fig4. 1 Security and Privacy in Opportunistic Networks

The Social-based Opportunistic Routing with Selfishness Detection and Incentive Mechanism (SORSI) Security and Privacy Framework, shown in Figure 4.1, displays how socioeconomic characteristics affect the way we develop security and privacy in opportunistic networks. The ESS mechanism helps to ensure better network security by providing mechanisms for identifying and isolating selfish nodes. Each node has an Encounter-Based Selfishness Score (ESS), which changes dynamically as a function of how often that node forwards messages. Nodes that continually refuse to forward messages will attract an increased ESS score and thus will be tagged as "selfish" nodes. Once identified as such, they will be excluded from forwarding any messages in the future and will thus be removed from participating in forwarding any messages for the protection of the opportunistic network against rogue nodes who misuse network resources. Nodes that are cooperative and take part in forwarding messages see a decrease in their rewards (ESS) and encourage continued cooperation through incentives. The HIBS feature of the framework is

designed to provide privacy and confidentiality to users. It does this by using the identity of the destination node as the public key for encrypting messages. Thus, there is no need for a centralized certificate authority to provide verification of the identities of nodes. Because of this feature, there is no way for intermediate forwarding nodes to decrypt or access the content of a message while it is being transferred. As shown in Figure 4.1, the combination of selfishness detection, incentives, and identity-based encryption protects users' data from being compromised in opportunistic networks.

Let the opportunistic network consist of a set of "mobile nodes"n. Secure communication enhancement is described by the following equations:

$$\lambda_{ij}(t) = \alpha\,\lambda_{ij}(t - \Delta t) + (1 - \alpha)\,I_{ij}(t) \qquad (4.1)$$

$\lambda_{ij}(t)$ is the exponentially weighted moving average (EMA encounter rate between node. $\alpha \in (0,1)$ is the EMA smoothing constant that controls memory of past observations, $\Delta t > 0$ is the discrete sampling interval, and $I_{ij}(t) \in \{0,1\}$ is the indicator function that node has a contact during the interval $[t - \Delta t, t]$ and 0 otherwise. It provides a temporarily smoothed estimate of contact frequency used in forwarding decisions. By using equation 5, k^{th} observed contact, and $N_{ij}\epsilon N$ is the number of observed contacts used to form the sample mean. This statistic quantifies expected contact length and informs link reliability.

$$\mu_i = \frac{v_i}{v_{max}} \qquad (4.2)$$

$\mu_i \in [0,1]$ is the normalized mobility factor for a node i, $v_i \geq 0$ is the instantaneous speed. $v_{max} > 0$ is a normalization constant representing the maximum expected speed in the environment. Lower μ_i corresponds to a more stationary node.

$$C_{i\to j} = \frac{B_{i\to j}}{T_{i\to j}} / max_{\,(p,q)} \frac{B_{p\to q}}{T_{p\to q}} \qquad (4.3)$$

$C_{i\to j} \in [0,1]$ is the normalized transmission capacity estimate from i to j; $B_{i\to j}$ is the instantaneous or estimated available bandwidth for the $i \to j$ link; $T_{i\to j} > 0$ is an estimate of the per packet or per bit transmission time over the link(s); , and the denominator is the

normalization factor taken as the maximum observed (B/T) ratio across all ordered node pairs (p, q). . This ratio captures relative throughput potential.

$$\beta_i = \frac{B_i^{avail}}{B_i^{max}} \tag{4.4}$$

$\beta_i \epsilon [0,1]$ is a node $i's$ buffer availability ratio; $B_i^{avail} \geq 0$ is the currently available buffer space, and $B_i^{max} > 0$ is the maximum buffer capacity. Values near one indicate abundant buffer resources.

$$\eta_i = \frac{E_i^{rem}}{E_i^{init}} \tag{4.5}$$

Here, $\eta_i \epsilon [0,1]$ denotes the normalized residual energy of node . $E_i^{rem} \geq 0$, remaining battery energy; and $E_i^{init} > 0$, initial battery capacity used for normalization. The term penalizes energy-poor nodes in routing decisions.

$$S_i = w_\lambda \tilde{\lambda}_i + w_d \tilde{\bar{d}}_i + w_\mu (1 - \mu_i) + w_\beta \beta_i + w_\eta \eta_i \tag{4.6}$$

$S_i \in [0,1]$ is the composite stability score for the node i; $\tilde{\lambda}_i$, and $\tilde{\bar{d}}_i$ are normalized versions of the encounter rate and average contact duration, respectively. Weights $w_\lambda, w_d, w_\beta, w_\mu \geq 0$ satisfy $\Sigma w = 1$ the term $1 - \mu_i$ converts normalized mobility into stability contribution. S_i Aggregates heterogeneous node attributes into a single relay candidacy metric.

$$R_{ij} = w_1 \tilde{\lambda}_{ij} + w_2 \tilde{\bar{d}}_{ij} + w_3 \frac{S_i + S_j}{2} \tag{4.7}$$

$R_{ij} \in [0,1]$ is the link reliability score between nodes i , and j; $\tilde{\lambda}_{ij}$ and $\tilde{\bar{d}}_{ij}$ are normalized encounter rate and the normalized mean contact duration for a pair, (i, j); S_i, S_j are the node stability score, and$w_1, w_2, w_3 \geq 0$ are the weighting coefficients with $\sigma_1 + \sigma_2 + \sigma_3 = 1$. R_{ij} captures pairwise forwarding robustness.

$$U_{i \to j}^{(m)} = w_1 R_{ij} + w_2 C_{i \to j} + w_3 \beta_j + w_4 \eta_j - w_5 \Phi_m \tag{4.8}$$

$U_{i\to j}^{(m)} \in R$is the forwarding utility of neighbor j for message m at node i. β_j , and η_j are neighbor $j's$ buffer and energy availability; $\Phi_m \geq 0$ is a message-specific penalty and $w_1, w_2, w_3 \ldots . w_5 \geq 0$ are non-negative weights chosen to balance terms. A larger U number indicates a more favourable forecast.

$$A(t) = \lceil A_0 \cdot (1 + \kappa\,(1 - \bar{S}(t))) \rceil \qquad (4.9)$$

Where $A(t) \in N$ is the adaptive copy count at time $.A_o \in N$, which is a baseline initial copy count. $k \geq 0$ is a control scalar setting sensitivity to network stability. $\bar{S}(t)$ =is the network average stability score computed from (7). the ceiling operator (⌈⌉)ensures an integer copy count. As $\bar{S}$ the number decreases, the algorithm increases A.

$$P_{i\to j} = \frac{\max\{U_{i\to j}^{(m)}, 0\}}{\epsilon + \sum_{k\in\mathcal{N}_i} \max\{U_{i\to k}^{(m)}, 0\}} \qquad (4.10)$$

$P_{i\to j}\epsilon[0,1]$ is the probability of selecting a neighbor j for forwarding at node $i; N$, where is the set of neighbors of i. $U_{i\to k}^{(m)}$. are utilises and $\epsilon > 0$ is a small constant to avoid division by zero. This probabilistic rule reduces redundant replication while biasing selection toward a higher utility neighbor.

$$D_{i\to d} = 1 - \prod_{t>0} (1 - \sum_{j\in\mathcal{N}_i(t)} P_{i\to j}\, D_{j\to d}) \qquad (4.11)$$

$D_{i\to d} \in [0,1]$ Denotes the estimated cumulative delivery probability from node i to destination; . The product is taken over forwarding opportunity epochs t; $N_i(t)$. The neighbor set at epoch t; $D_{j\to d}$ is the recursive delivery probability from neighbor j to d. the multi-hop success probability under the forwarding policy.

$$ETX_{i\to d} \approx \frac{1}{\epsilon + D_{i\to d}} \qquad (4.12)$$

$ETX_{i\to d} > 0$ is an Expected Transmission Count approximation for delivery from i to d; $\epsilon > 0$ is a small regularization constant. A smaller ETX indicates fewer expected retransmissions and thus a preferred route.

$$\Omega(t) = \frac{\sum_{m\in\mathcal{M}(t)}(\text{copies}_m(t)-1)}{|\mathcal{M}(t)|} \tag{4.13}$$

Here $\Omega(t) \geq 0$ is the instantaneous replication overhead ratio at time t. $Copies_m(t)$, which denotes the instantaneous number of copies of measures, $m.\Omega$ measures average replication beyond the baseline single copy.

$$\bar{L} = \frac{1}{M_D}\sum_{m\in\mathcal{D}}(t_m^{\text{recv}} - t_m^{\text{sent}}) \tag{4.14}$$

Where$\bar{L}$ is the sample mean latency across delivered massages; D represents a set of "delivered messages"; $m_D = |D|$ is the delivered message count; and t_m^{sent}, t_m^{recv} are the send and receive timestamps for the message m. This metric evaluates timeliness under the protocol.

$$P_{overflow,i} = 1 - \sum_{k=0}^{B_i^{max}} \frac{(\lambda_i T)^k e^{-\lambda_i T}}{k!} \tag{4.15}$$

$P_{overflow,i}\epsilon[0,1]$ is the probability of buffer overflow at node i over window $T > 0$ under a Poisson arrival assumption; $\lambda_i \geq 0$ is the message arrival rate to node i , and B_i^{max} is the integer buffer capacity. This expression guides congestion-aware forwarding and drop policies.

$$ESS_i(t+1) = \rho\, ESS_i(t) + \delta \cdot 1_{\{forw_i(t)=0\}} - \phi \cdot 1_{\{forw_i(t)=1\}}$$

(4.16)

$ESS_i(t) \in R_{\geq 0}$ is the "ESS" for node i at epoch, $t; \rho \in (0,1)$ is a decay factor modelling;$\delta > 0$ is the penalty increment when node i refuses to forward at epoch, t; $\phi > 0$ is the reward decrement applied when node i corporates and $1_{\{forw_i(t)=0\}}$ denotes the indicator function. Larger ESS indicates greater measured selfishness.

$$C_i = max\ \{0,\ 1 - \frac{ESS_i}{ESS_{max}}\} \quad (4.17)$$

$C_i \in [0,1]$ is the cooperation index derived from ESS; $ESS_{max} > 0$ is a design parameter representing the maximum ESS used for normalization. This maps high selfishness to low cooperation scores used in forwarding decisions.

$$\widetilde{U}_{i\to j}^{(m)} = C_j\, U_{i\to j}^{(m)} - \xi\, ESS_j \quad (4.18)$$

$\widetilde{U}_{i\to j}^{(m)} \in R$ is the trust adjusted forwarding utility; C_j and ESS_j are the cooperation index and ESS of the neighbor j; $\xi \geq 0$, which is a penalty weight scaling direct ESS subtraction. This composite disincentivizes forwarding to selfish nodes while rewarding cooperative ones.

$$c = Enc_{\ HIBS}(M,\ PK_{ID_d}) \quad (4.19)$$

c denotes the ciphertext produced by a hierarchical Identity Based Security (HIBS) encryption operation; m is the plaintext message; and PK_{ID_d} denotes the HIBS public key derived deterministically from the identity ID_d of the destination d. The HIBS primitive allows intermediate nodes to forward ciphertext without knowledge of private keys, ensuring end-to-end confidentiality tied to identity.

$$P_{dec}(d) = \theta_{KM}.(1 - P_{revok}(d)) \quad (4.20)$$

$P_{dec}(d) \epsilon [0,1]$ The modelled probability that the destination d can successfully obtain its private key and decrypt the ciphertext $c.\theta_{KM} \epsilon [0,1]$ is the estimated key management system reliability, and $P_{revok}(d) \in [0,1]$ is the keying material that d has been revoked. This model secures delivery feasibility in the presence of dynamic key management.

$$M_{i\to j}^{(m)} = w_1 \widetilde{U}_{i\to j}^{(m)} + w_2 D_{j\to d} - w_3 ETX_{j\to d} + w_4 log\ (1 + P_{dec}(d)) - w_5 E_{i\to j}$$

(4.21)

It $M_{i\to j}^{(m)} \epsilon R$ is the composite decision metric for selecting a neighbor j as the next hop and bound for "destination," d; and $w_1, w_2, \ldots . w_5 \geq 0$ the weights chosen to balance reliability, timeliness, security and energy. The logarithmic term compresses diminishing returns of increasing decryption probability.

$$E_{i\to j} = \zeta_{tx} \cdot s_m \cdot (\frac{d_{ij}^{\beta}}{G_{ij}}) + \zeta_{proc} \quad (4.22)$$

$E_{i\to j}$ is the expected energy cost to transmit a message m from i tp $j, \zeta_{tx} > 0$ is a transmission energy coefficient; $s_m > 0$ is the message size in bits; $d_{ij} \geq 0$ is the physical separation between i and j; $\beta \geq 1$ denotes path loss exponent; $G_{ij} > 0$ is an estimate of channel gain between i and j; and $\zeta_{proc} \geq 0$ accounts for processing energy. This expression captures energy trade-offs in forwarding:

$$\max_{x_{ij}\in\{0,1\}} \sum_{j\in\mathcal{N}_i} x_{ij}\, \mathcal{M}_{i\to j}^{(m)} \quad \text{subject to} \sum_{j\in\mathcal{N}_i} x_{ij} \leq L_i^{\text{rem}}, \beta_i \geq \beta_{\min}, \eta_i \geq \eta_{\min} \quad (4.23)$$

Node i solves a local constrained selection problem at an encounter; $x_{ij} \in \{0,1\}$ it is a binary decision variable indicating whether to forward to a neighbor $j. L_i^{rem} \in N$ is the remaining allowed number of message copies that i can be distributed for the message $m. \beta_i$ and η_i are node $i's$ buffer, and energy availability, and β_{min}, η_{min} are designer specified minimum resource thresholds. The constraint enforces local resource feasibility.

$$max\ \ J = \lambda_D\, DR^- - \lambda_\Omega\, \Omega^- - \lambda_L\, L^- - \lambda_E\, E^-_{cons} + \lambda_S C^- \quad (4.24)$$

J is a global scalar objective representing system utility to be maximized in aggregate; $DR\epsilon[0,1]$ is the long-term network delivery ratio; Ω^- is the long-term average replication overhead. E^-_{cons} is the average energy consumed per node or per message. C^- is the network average cooperation index. $\frac{1}{|N|}\sum_i \quad C_i$ and $\lambda_D, \lambda_\Omega, \lambda_L, \lambda_E, \lambda_S \geq 0$ are Lagrange style weights

that specify the designer's trade-offs between delivery performance, overhead, latency, energy, and cooperation. Pseudocode for Secure Communication Environment is presented in Algorithm 2.

4.2 Model

Identity-Based Cryptography

The proposed new approach to create an opportunistic network uses an Identity-Based Cryptography (IBC) model, allowing for the establishment of secure, lightweight, and highly scalable communications while also providing a complete solution to a problem that has been created by using untrusted centralised Certificate Authorities. Opportunistic networks have many of the same issues as other types of communications networks, such as not having continuous access to a trusted infrastructure due to intermittent connectivity and dynamic topologies, therefore making it impractical to use traditional Public Key Infrastructures due to the large amount of overhead and complexity to manage. The new approach introduced in this work implements a Hierarchical Identity-Based Security (HIBS) model. In Fig 4.2 depicts Hierarchical Identity-Based Security (HIBS) model

The HIBS method uses a unique identity of each node to generate its public key (node ID); therefore, in the HIBS method, a message can be encrypted based on the identity of your destination node instead of the destination node's public key. In this way, sending an encrypted message from one node to another over the Internet is possible even if there is no direct connection to the Internet at that time. During the store-carry-forward method, all encrypted messages are sent as encrypted Ciphertext through every intermediate relay node; therefore, because the relay nodes only have access to the encrypted message, there is no way for them to decrypt it. Because of this fact, only the authenticated destination node may have access to the plaintext of the message, therefore eliminating any risk of unauthorized access or data breach through any of the relay nodes [215].

A significant benefit of identity-based architectures is that they can scale more efficiently than other architectures while alleviating the burden of key management on the resource-constrained opportunistic networks, thereby enabling a broad range of users to take advantage of an IDCA. The elimination of certificate exchanges and certificate verification requirements also lowers the overall computational and communication costs of the proposed identity-based cryptographic model while maintaining a high level of security, privacy, authentication, confidentiality, and data integrity. Thus, identity-based cryptography will play a crucial role in providing a secure and private opportunistic routing network that incorporates SORSI-HIBS functionality.

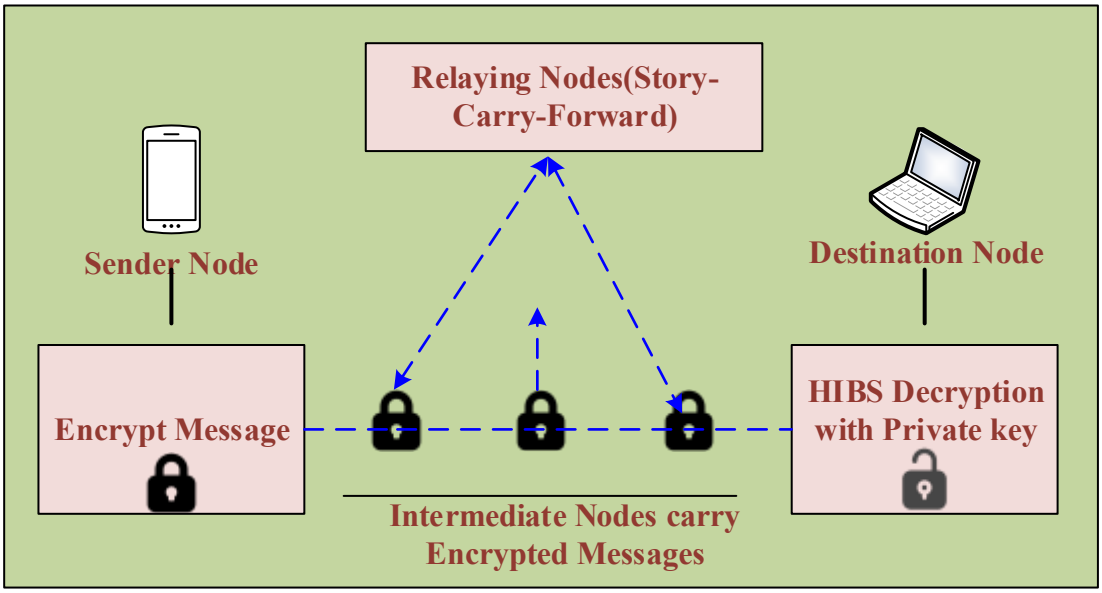

Fig4. 2 Hierarchical Identity-Based Security (HIBS) model

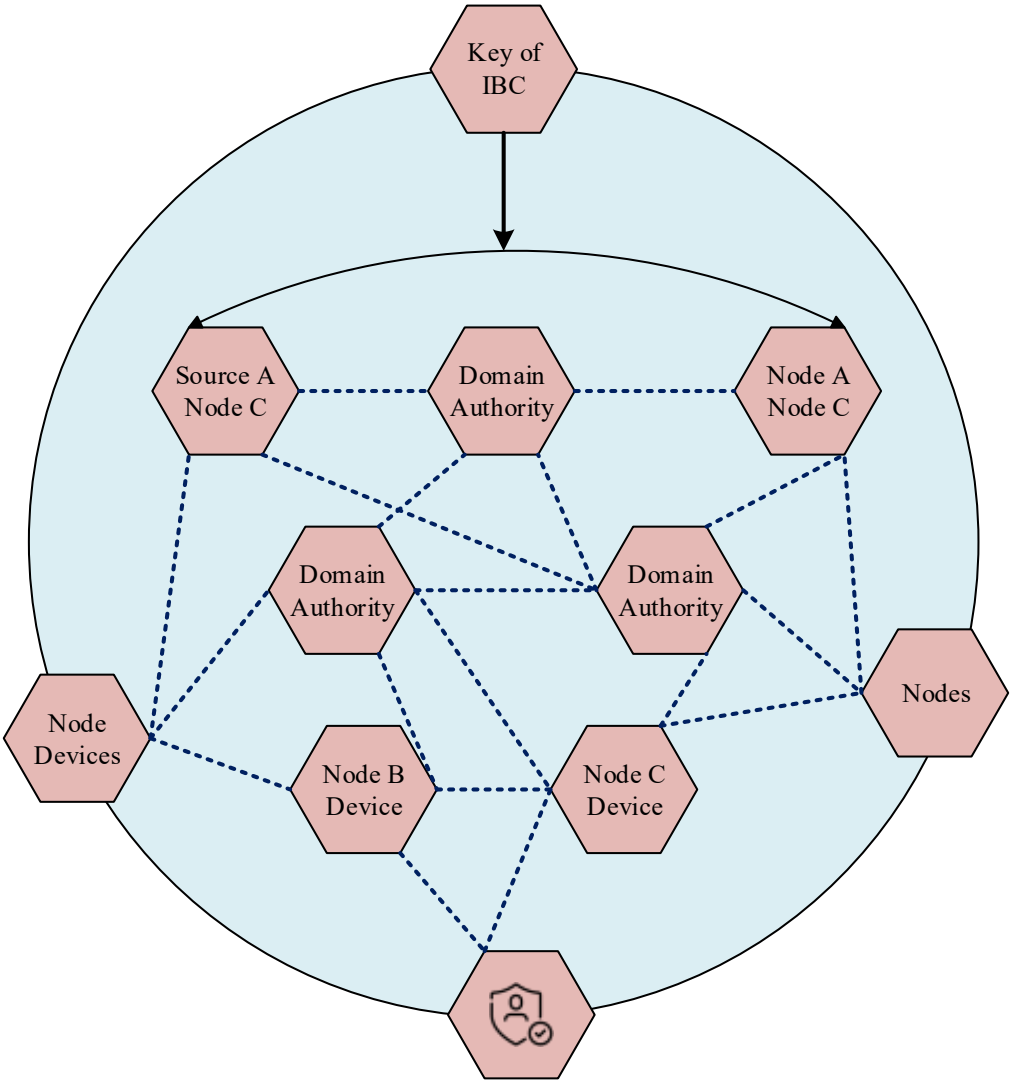

Fig4. 3 Identity-Based Cryptography

The structured identity-based cryptographic system model is depicted in Figure 4.2 as employing a hierarchical framework consisting of multiple levels of authorities (root authority), private key generators delegated by the root authority, an entity of "participants", and a group of devices referred to as "opportunistic relays". As such, this model is able to provide secure communication between the nodes when centralised certification authorities are not available or maintained, and does so in an environment where devices/repeater access will not remain continuous.

The R-PKG (Root Private Key Generator) creates global public parameters and a master secret key that initializes the system. Public parameters are shared by all nodes in the network; however, the master secret key is held securely at the root authority level. In comparison with today's traditional PKI-based systems, there are no certificates that are

issued or validated, thus greatly reducing the reliance on centralized infrastructure and management overhead.

In addition to the root authority, domain-level or area-level Private Key Generators (PKGs) provide decentralized operation and scalability. PKGs create private keys based upon the identity of subordinate nodes, which can include node identifiers, email addresses, or any other ID for a specific network. By delegating the Key Generation Hierarchically, the chance of experiencing a “single point of failure” is decreased, while providing an efficient means of scaling as the network continues to grow.

Every participating device in the opportunistic network gets its own private key safely during a one-time registration period. After receiving their private key, nodes are secure in the ability to decrypt messages that are addressed to their identity. When sending a message, the source node will encrypt that message using the destination node’s identity as its public key and the public parameters of the system; at no time during the creation or sending of the message does the source node need to interact with the destination node or a trusted third party. This characteristic of the encryption process makes it ideal for use in the method of store-carry-forward communications.

Authentication (the process of verifying the identity of someone who provides messages) and verification of the integrity of those messages are also supported by the hierarchical identity-based model. Because every message is 'cryptographically bound' to the sender's (the sending node's) identity, any receiving node may independently verify that it originated from a specific sender. This feature enhances SORSI's level of trust, since it provides an extra layer of trust (i.e., via cryptographic techniques) in addition to SORSI's level of trust created through behavioral evaluations, and thus greatly enhances the security of an opportunistic network.

The HIBS (Hybrid Identity-Based Security) model, detailed in Figure 4, features a lightweight key management scheme that reduces the computational complexity, storage needs, and communication overhead by removing the need for certificate exchanges,

revocation lists, and ongoing validation of keys. As such, HIBS is particularly well-suited for mobile and IoT devices with limited storage, processing power, and battery life.

The proposed Hybrid Identity-Based Security model outlined in a secure, scalable, and efficient platform for enabling opportunistic networking by integrating with a stability-aware routing strategy and the SORSI framework to provide secure end-to-end communication while protecting user privacy. In addition, the integrated design provides resilience against malicious and selfish node behavior and addresses the previously identified challenges of security and scalability associated with opportunistic networking frameworks. In Fig 4.3 depicts Identity-Based Cryptography

Social-based Routing

Routing using social factors takes advantage of social actions and behaviour within the network (opportunistic networks) to increase routing efficiency. Traditional Routing methods only consider the topology and/or movement prediction of the network, whereas Social Routing considers social relationships, how often each node comes into contact with the other nodes, and levels of cooperation between nodes to make intelligent forwarding decisions. As a result, Social Routing has proven to be a successful routing type for many types of opportunistic networks formed around the behaviours of people, where people will follow predictable patterns of social connection.

A new system of routing that relies on the social network of a node uses a new algorithm called the Social-based Opportunistic Routing for Selfishness detection with Incentives (SORSI). The SORSI system uses a node's ESS (Encounter-based Selfishness Score) to determine whether it is "good" or "bad" based on how often it forwards messages. Good nodes are rewarded while bad nodes are punished for not cooperating. The SORSI system encourages good behaviour and discourages negative behaviour.

Decisions regarding routing paths are made based on determining which nodes are more likely to behave cooperatively with other nodes and therefore have the highest trust and encounter reliability. Routing decisions are then made based on those cooperative nodes,

thereby increasing the chance of successfully delivering a message and eliminating the possibility of duplicating messages unnecessarily [216-218]. By solution path routing decisions using social awareness of Nodes, the proposed network architecture has resulted in a significant reduction in routing overhead, significantly higher delivery ratios, and improved network stability over time. In addition, through the combination of routing decisions that consider social awareness and selfish behaviour detection/incentives, routing can occur more easily and efficiently, ensuring secure and reliable forwarding of data in WSN dynamically opportunistic environments.

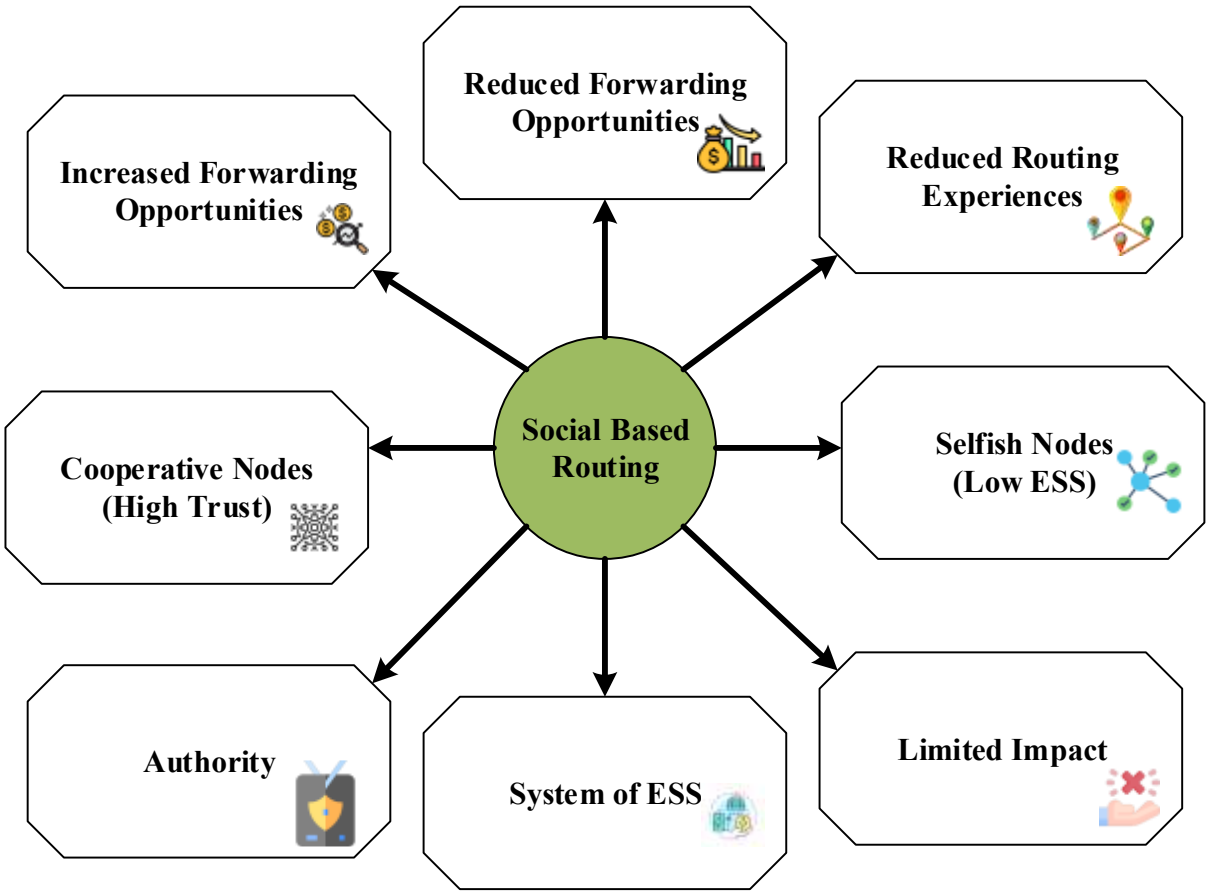

Fig4. 4 Social-based Routing

More specifically, when employing social-based opportunistic routing models, it is assumed that people do not randomly move throughout the world nor perform random acts of kindness; instead, people tend to move according to known social structures (such as community groups) and to meet in the same places repeatedly. By measuring the social

behavior of their respective user base, social-based opportunistic routing models can provide a better estimate for future forwarding opportunities than traditional mobility-based models.

A number of performance metrics - including frequency of encounters, duration of contact, degree of social similarity, and degree of centrality within the network - are all used to define the routing decisions and capture the social characteristics of the users within the routing protocol. Several currently available social routing protocols employ community detection and social centrality techniques to improve the delivery of messages. While these protocols do improve the performance of message delivery, they are typically based on the assumption that all nodes will behave cooperatively with one another and do not adequately account for the presence of selfish or malicious behaviors from nodes. In a real-world opportunistic environment, there are many situations in which nodes will not forward messages (e.g., because of limited resources, energy constraints, or deliberate non-cooperation). This presents a significant challenge to social-based routing, as without cooperation being strictly enforced, social-based routing cannot be relied upon to be effective.

We recognize that the use of "Selfish Behaviour Detection" as a way to determine trust is a limitation in this research. To compensate for this shortcoming, we are creating a new model called SORSI (Social Organisation and Resource Sharing Interface) that includes methods for identifying selfish behaviours within a cooperative reward structure. In SORSI, the viewpoint of each node regarding how they engage with other nodes is evaluated using a Selfishness Score Based on Encounter (ESS). The ESS is a dynamic, real-time measure based on the forward behaviour of each node, which occurs during encounters (the process of interacting with another node). Since nodes who frequently forward messages during encounters will be considered as acting cooperatively, their trust scores will be higher, while nodes who frequently fail to forward or drop messages will be judged to be acting in a selfish manner. The evaluation of the forwarding behavior of nodes in real time gives the routing mechanism the flexibility to adjust to fluctuations in forwarding behavior as they happen.

SORSI also uses incentive structures to support long-term cooperation among network nodes. Nodes that participate cooperatively are rewarded with increased forwarding opportunities (or) are assigned a greater routing priority. In contrast, selfish nodes will receive reduced routing experiences as a consequence of their selfish actions, thereby limiting their impact on the overall network performance. By balancing these two incentives, SORSI is able to create an environment that encourages equitable behaviour while still being able to maintain high levels of routing efficiency.

Another benefit of using social-based routing using SORSI is that it decreases the number of unnecessary message replicates. Rather than using either flooding methods or static quotas, SORSI selects only those nodes with high social trust and high reliability for forwarding messages to reduce the number of message replicates that are sent through the network. The reduction in the number of replicated messages results in a considerable reduction in the amount of resources that are used for routing, including the buffer space required, the amount of power consumed, and the use of additional packet overhead, which is an important factor when developing an opportunistic routing protocol.

In addition, combining self-aware (social) nodes with selfishness detection of non-cooperative nodes results in a greater degree of reliability and survivability within the network as a whole. When routing resources from a node using only its cooperative behaviours, the overall outcome of that resource's use will allow for greater network resilience due to the reduction in both node mobility and malicious activity that disrupts other nodes within the network. Over time, routing will become more predictable and will develop into a stable forwarding route, as a result of the establishment of trust-based social connections, thereby increasing the delivery of data in rapidly changing environments.

The application of the proposed social-based routing strategy can be extended to a variety of real-world applications. For example, this routing approach could be used for disaster recovery operations, vehicle-based networks, smart city infrastructure, wearable networks, and IoT-based opportunistic systems. These applications all share the common

characteristic that social behaviour and interaction patterns naturally shape communication availability, therefore creating a unique opportunity where the use of social-based routing will perform quite well with the addition of incentive-based enforcement.

Therefore, this work demonstrates that the combination of social behaviour awareness, trust-based evaluations, and incentive-based co-operation can increase the effectiveness of routing in opportunistic networks. By addressing both routing performance and the behaviour of the nodes at the same time, the proposed routing approach provides a scalable and secure mechanism for ensuring that data can be reliably disseminated throughout highly dynamic and resource-limited opportunistic networks.

4.3 Algorithm (with Time and Space Complexities)

Algorithm 2: Secure Communication Environment (SORSI-HIBS)

Data: Node encounter records {Contact logs, forwarding events}

Input: Selfishness update factors (γ, ρ), cooperation threshold, HIBS identity Keys $K(ID)$

Result: Secure and cooperative message forwarding in the opportunistic network.

1. Initialize Encounter-Based Selfishness Score (ESS) for all nodes

2. Compute the initial cooperation index C_i for each node using ESS

3. Assign identity based public key $K(ID)$ through HIBS

4. While (Message forwarding continues) do

5. Update ESS using γ and ρ based on forwarding or refusal actions

6. Recomputed C_i and classified nodes as cooperative or Selfish

7. Encrypt the message using the HIBS public key to form

Ciphertext c.

8. Select only cooperative nodes for forwarding based on $C_i \geq \tau$

9. Validate forwarding node through encounter history to

Prevent replay

10. Forward the encrypted message c through a trusted

Cooperative nodes

11. Replace any low-cooperation node with the next best

Cooperative neighbor.

12. End while

13. Return securely delivered message and updated

Cooperation indices.

Time Complexity Analysis

1. Updating ESS for each encounter → $O\ (1)$

2. Recomputing the cooperation index for N nodes → $O(N)$

3. Selecting cooperative neighbors among k nodes → $O(k)$

4. Identity-based encryption/decryption (HIBS) → $O\ (1)\ per$

Message

5. Forwarding m messages → $O(m)$

$$T_{SORSI-HIB} = O(N + K + m)$$

Space Complexity Analysis

1. ESS table for all nodes → $O(N)$

2. Cooperation index and reputation history → $O(N)$

3. HIBS public/secret key storage → $O(N)$

$$S_{SORSI-HIBS} = O(N)$$

Through using the SORSI-HIBS algorithm, secure and cooperative message forwarding will be accomplished in opportunistic networks. This will be achieved by using Selfish Node Detection (i.e., Selfish Node Identification as defined by SORSI) in conjunction with Identity Based Cryptographic Security (i.e., Hierarchical Identity Based Security) to provide both methods for cooperation enforcement as well as confidentiality of data.

At the beginning, all nodes in the network are given an Encounter-Based Selfishness Score (ESS) that reflects their past behavior of forwarding messages based on the records of their encounters and events when they forwarded messages. The ESS values are then utilized to calculate each node's initial cooperation index Ci (Ci denotes cooperation index), representing the extent to which they will forward messages. Ultimately, the nodes with higher cooperation indices will be viewed as being more dependable when it comes to routing messages.

The HIBS framework assigns an identity-based public key for each node to ensure secure communication. Each node in this method uses its ID as its own Public Key, and it does not require a Certificate Authority. By not requiring a Certificate Authority, the amount of overhead associated with Key Management is less. This method is especially beneficial for infrastructure-less opportunistic networks.

When message forwarding is enabled, an algorithm is used to update the ESS values based on a set of selfishness update factors γ. When a node decides to forward a message, its ESS will be decreased, but when it decides not to forward a message, its ESS will be increased. This change in ESS will cause a recalculation of the cooperation index Ci, which will allow for the dynamic classification of nodes as cooperative or selfish, based on the predefined cooperation thresholdτ.

When a forwarding node's cooperative index falls below the threshold, it will be immediately substituted by the subsequent best cooperative neighbor. This dynamic replacement method provides continued message forwarding without interruption while protecting the security and trust of the nodes in the network. This replacement procedure will continue until the message has been delivered successfully to the endpoint.

Finally, after generalising the secure delivery of a message together with the associated updates to the cooperation index, the algorithm is able to perform Trust Evaluation on the cooperation of nodes through adaptive and continual processes.

The main operations of the SORSI-HIBS Algorithm influence the SORSI-HIBS Algorithm's time complexity. Updating the ESS for each encounter with an agent occurs in constant time $O(1)$. For recomputing the cooperation index for all N nodes, we incur $O(N)$ time. Selecting cooperative neighbours from k candidates will require $O(k)$ time. Encrypting and decrypting HIBS messages using Identity-Based Encryption occurs in constant time per message $O(1)$. When forwarding a total of mmm messages, we have the following overall complexity:

$$T_{SORSI-HIB} = O(N + K + m)$$

The major contributor to the space complexity is the storage of trust/security information. The amount of space required to maintain the ESS table for each of the nodes is O(N). The space necessary to store the cooperation index and reputation history will also be O(N). Finally, the space to store all nodes' identity-based public/private keys will be O(N). As such, the total space complexity will be:

$$S_{SORSI-HIBS} = O(N)$$

This certifies that the suggested secure routing system is a memory-efficient method and also works well for opportunistic networks with large scale.

4.4 Experiment Setup (with ONE Simulator)

4.4.1 Simulation Setup

The section proposes a novel approach for secure and privacy protocols, as well as being set up for simulation. To simulate the proposed research method, the Java version JDK 21.0.5 was used [209].

Table 4.1 displays the System specification.

Table4. 1 System specifications

Hardware Specification	Hard disk	512 GB
	RAM	16 GB
Software specifications	Simulation tools	Java Version: JDK 21.0.5
	OS	Windows 11(64- bit)

In Table 4.2, Simulation parameters are presented. The category Interfaces, Host Groups, mobility, Routing protocols, security, and optimization is provided.

Table4. 2 Simulation Parameters

Category	Parameter	Value(s)
Scenario	Name	Proposed Approach
	Simulate Connections	true
	Update Interval	0.1 s
	End Time	43200 s (12 h)
Interfaces	btInterface Type	Simple Broadcast Interface
	btInterface Speed	250 kbps
	btInterface Range	40 m
	highspeedInterface Type	Simple Broadcast Interface
	highspeedInterface Speed	10 Mbps
	highspeedInterface Range	10 m
Host Groups	Group Router	STCESW Router
	Group Buffer Size	5 MB (default), 50 MB (trams)
	Group Speed	0.8–2.5 m/s (pedestrians), 2.7–13.9 m/s (cars), 7–10 m/s (trams)
	Group Wait Time	0–120 s (default), 10–30 s (trams)
	Group Interfaces	1 (default), 2 (trams with bt + high-speed)
	Group Message TTL	20000 s
	Group Sizes	30 (p), 30 (c), 30 (w), 3 (tram3), 3(tram4), 4 (tram10)

Mobility	Movement Model	Shortest Path Map-Based Movement, Map Route Movement (trams)
	World Size	4500 × 3400 m
	Warmup	1000 s
	Map Files	roads.wkt, main_roads.wkt, pedestrian_paths.wkt, shops.wkt
Events	Event Generator Class	Message Event Generator
	Interval	10–18 s
	Message Size	500 KB – 1 MB
	Hosts	0–99
	Prefix	M
	TTL	20000 s
Reports	Reports	Message Delivery Report, Message Delay Report, Message Copy Count Report, Contact Times Report, ConnectivityONEReport
	Report Directory	reports/
	Granularity	10
Routing Protocols	ProphetRouter Time Unit	30 s
	SprayAndWait Copies	6
	SprayAndWait Binary Mode	true
	STCESW Base	10

	Copies	
	STCESW Stability Weight	0.35
	STCESW Capacity Weight	0.65
	STCESW Selfish Threshold	0.3
	STCESW Initial Reputation	0.5
	STCESW Observation Window	10
	STCESW Credit Reward/Penalty	+10 / -5
	SORSI Detection Threshold	0.30
	SORSI Reward Credits	1 per forward
Security (HIBS)	Enabled	true
	Signature Only	true
	Key Algorithm	RSA
Optimization	Cell Size Multiplier	5
	Randomize Update Order	true
GUI	Underlay Image	helsinki_underlay.png
	Offset	64, 20
	Scale	4.75

	Rotate	-0.015
	Event Log Panel	100 events

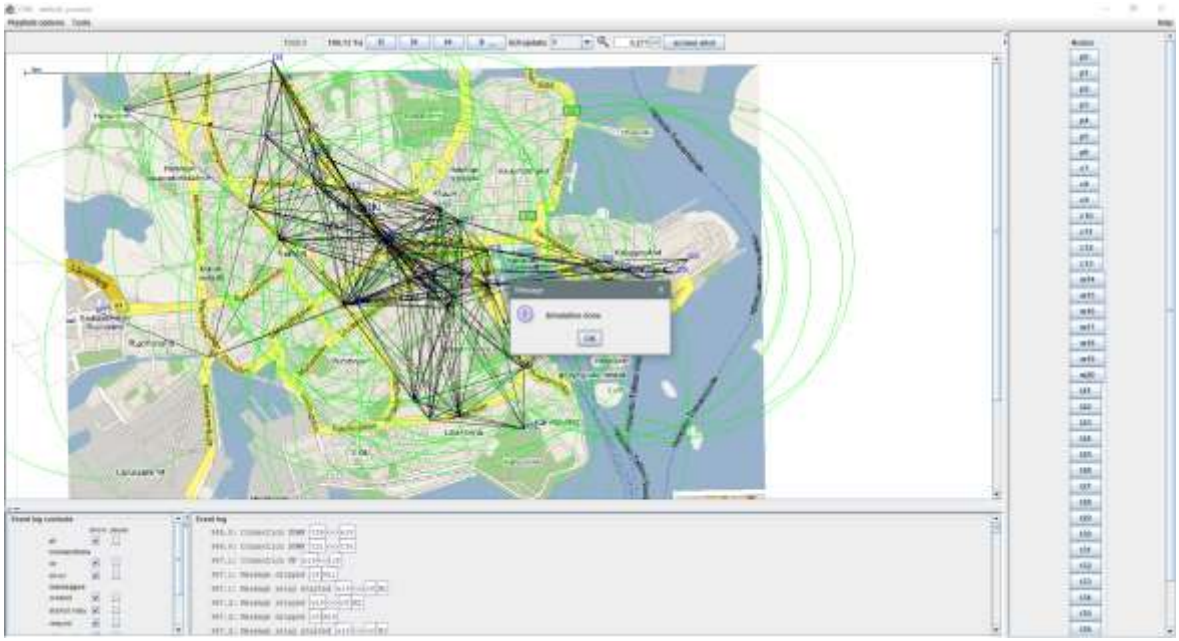

Fig4. 5 One Simulation Parameter Networks

In Fig. 4.2, “simulation network environment” is configured in realistic contact patterns, node mobility, and wireless communication properties to closely represent real-world dynamic network conditions, and the opportunistic network is constructed with 100 nodes.

4.4.2 Comparative analysis

The proposed technique has been compared against a variety of current techniques within these three specific areas; i.e. the relationship of time to delivery ratio, cumulative probability to average latency, and time to overhead ratio (%) in comparison to both ECSUO (Edge community service in opportunistic social networks) and CATR (Context-Aware Trust and Reputation Routing Algorithm). The results indicate that the proposed methodology offered superior performance as well as very high accuracy compared with the other techniques tested.

4.4.2.1 Number of Nodes Vs Delivery Ratio (%)

The Delivery Ratio (DR) provides a measure of the performance of the Secure Routing Framework (SRF) in terms of how many packets were delivered from the source to their destination successfully. With increasing numbers of nodes in Secure Opportunistic Routing (SOR), DR can decrease due to the delays associated with authenticating nodes and the overhead of encryption, as well as because SOR restricts packet forwarding to trusted nodes only. However, usage of the New SOR for Hybrid Identity-Based Signature (SORSI-HIBS) continues to show a high DR even with increased network density. The DR is improved because if a node is not cooperative, it will not be used in the routing path, while cooperative nodes will not be used to route packets to a malicious or unreliable destination. This enables the secure routing framework(s) in SORSI-HIBS to ensure that reliable data delivery occurs while maintaining the integrity and trust in the network.

Table4. 3 Number of Nodes Vs Delivery Ratio (%)

Number Of Nodes	Delivery Ratio (%)	
	SORSI-HIBS (Proposed)	CATR (Existing)
50	60	50
100	65	53
150	70	58
200	75	60
250	80	65
300	85	70
350	90	75
400	95	78

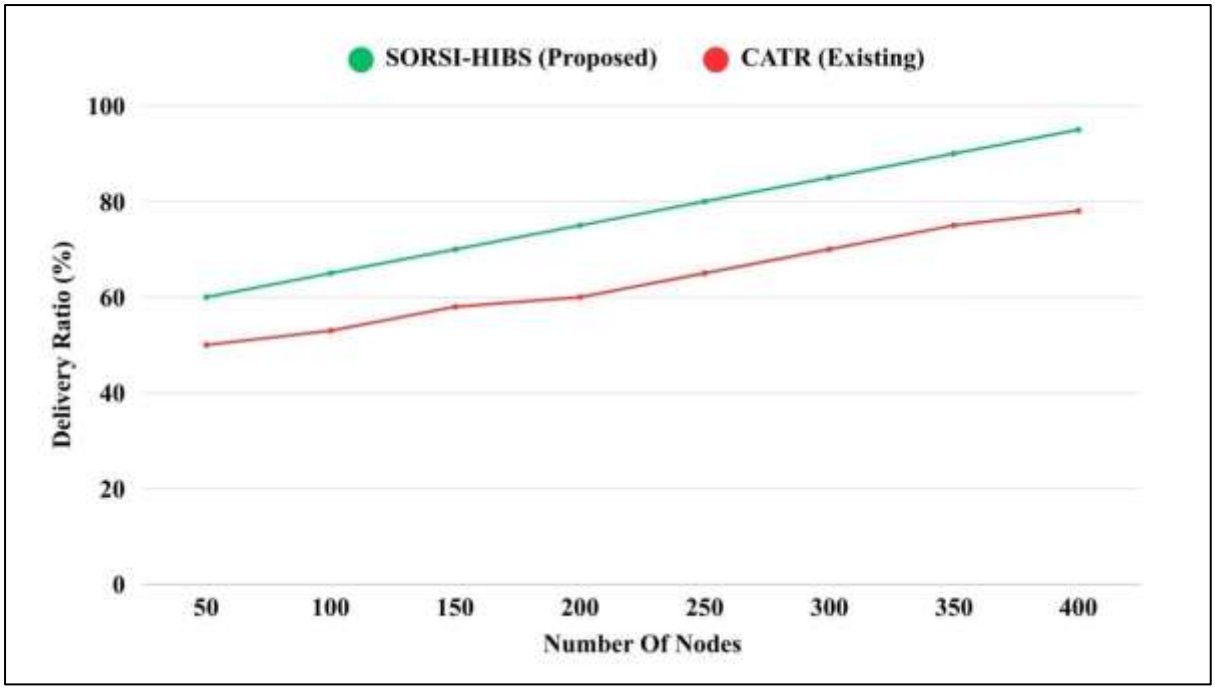

Fig4. 6 Number Of Nodes Vs Deliver Ratio (%)

In Table 4.3 and Fig. 4 .3, the delivery performance of Secure SORSI-HIBS against Existing CATR Protocols has been shown graphically. The graph indicates that with an increase in node density, the successful delivery rate improves for both protocols. However, SORSI-HIBS is always ahead of CATR. For example, at a 50-node density, SORSI-HIBS achieved a delivery ratio of 60% while CATR achieved a delivery rate of 50%. At 400 nodes, the delivery ratio for SORSI-HIBS was 95% while that of CATR was 78%. This shows that SORSI-HIBS provides considerable resistance to security threats, and it has a higher successful delivery ratio than does CATR.

4.4.2.2 Number of Nodes Vs Average Latency(s)

Average Latency is a measure of how long it takes to get a message from one end of a network to the other end of that network when it is sent over a secure network route. As the number of Nodes increases, the average Latency increases due to several factors, which include encryption, authentication, available Buffer Space, and multiple hops that the message must take to reach its destination. The proposed Secure Routing approach reduces average Latency through the use of Lightweight Identity-Based Encryption and the Selective Forwarding of Messages utilizing Multi-Hop Routing between Cooperative Nodes. The

elimination of the need for Certificate Verifications and Centralized Key Distributions by HIBS means that the amount of time a message takes to be processed cryptographically is drastically reduced. In addition, by preventing the use of Selfish Nodes and selecting Stable Cooperative Relays, unnecessary Multiple Hops and delays are reduced. As such, average latency remains relatively low under conditions of dense Networking, indicating the efficiency of the proposed routing design.

Table4. 4 Number of Nodes vs Average Latency(s)

Number Of Nodes	Average Latency(s)	
	SORSI-HIBS (Proposed)	CATR (Existing)
50	5	6
100	8	8
150	10	15
200	15	18
250	20	20
300	23	25
350	25	30
400	27	34

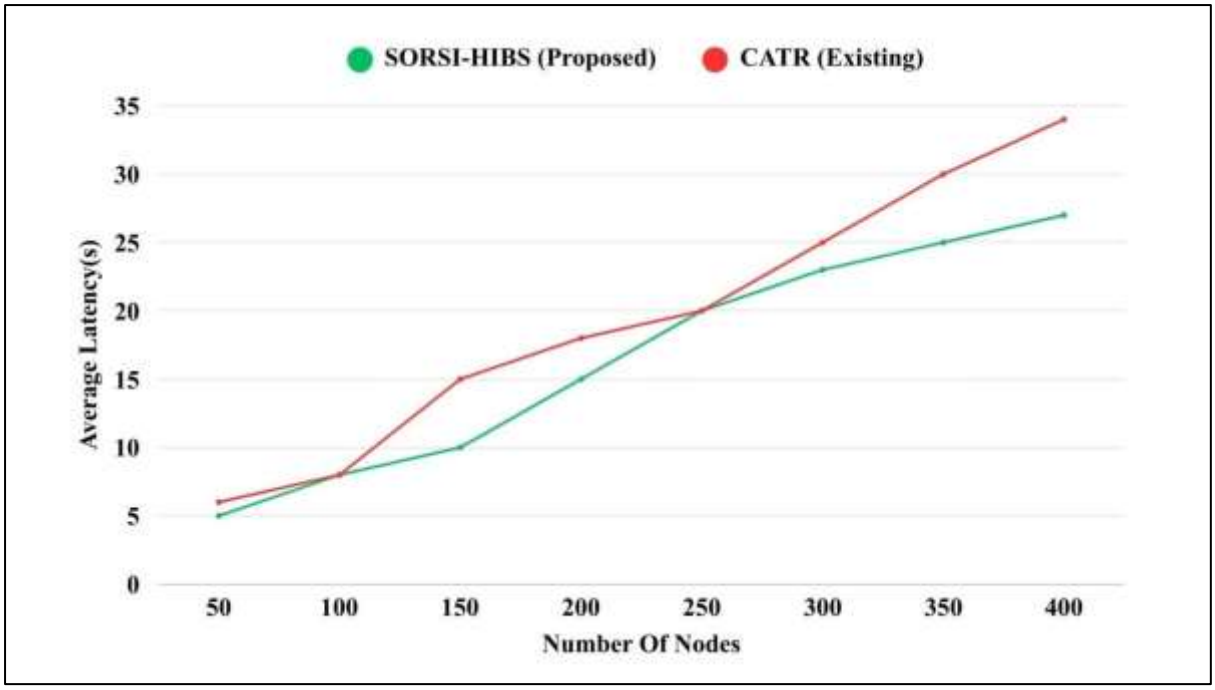

Fig4. 7 Number Of Nodes Vs Average Latency(s)

In Table 4.4 and Fig. 4 .4, the effect of increasing the number of nodes on both routing protocols is to cause an increase in latency. This increase in latency is due to an increase in the amount of contention and a buffering delay from all the new nodes trying to communicate with each other. However, when looking at SORSI-HIBS, we see that the maximum impact of increasing the number of nodes is smaller than for CATR. The primary reason for this is that SORSI-HIBS employs an efficient secure authentication mechanism, and therefore has a lower verification overhead than other routing protocols. In addition, as more and more nodes join, SORSI-HIBS will continue forwarding packets with less processing time than CATR. For example, at 400 nodes, SORSI-HIBS has a latency of 27 seconds, while for CATR, the latency is increased to 34 seconds. difference in performance exhibited by the two routing protocols shows how SORSI is capable of delivering lower latency and maintaining reliable communication in a very high density opportunistic environment.

4.4.2.3 Number of Nodes Vs Overhead Ratio (%)

An overhead ratio is simply the costs associated with using secure message forwarding which are incurred by the added route. Included in this cost are the costs of sending messages from one secure location to another, authentication message, and any repeated transmissions. The result of using traditional secure routing protocols is often rapid increases in overhead as node densities increase due to the repeated verification of received packets and the multiple copies of some messages created by the system. In contrast, while the number of nodes increases, the proposed secure routing framework, through the implementation of various techniques outlined above (such as selective message forwarding, encounter-based trust evaluations, and controlled replication of messages), results in a slower rate of increase in the overhead ratio. By only forwarding packets to those nodes that are trust-based and eliminating repeat transmissions, there is a significant reduction in the overhead created by sending packets to non-cooperative nodes, and therefore reducing packet transmission for all nodes. Overall, these findings indicate that the secure routing design is lightweight, scalable, and therefore the best design available for use in very high-density opportunistic networks.

Table4. 5Number of Nodes Vs Overhead Ratio (%)

Number Of Nodes	Overhead Ratio (%)	
	SORSI-HIBS (Proposed)	CATR (Existing)
50	8.0	10.0
100	7.8	9.8
150	7.6	9.7
200	7.4	9.5
250	7.3	9.3
300	7.2	9.2
350	7.1	9.1

400	6.0	8.0

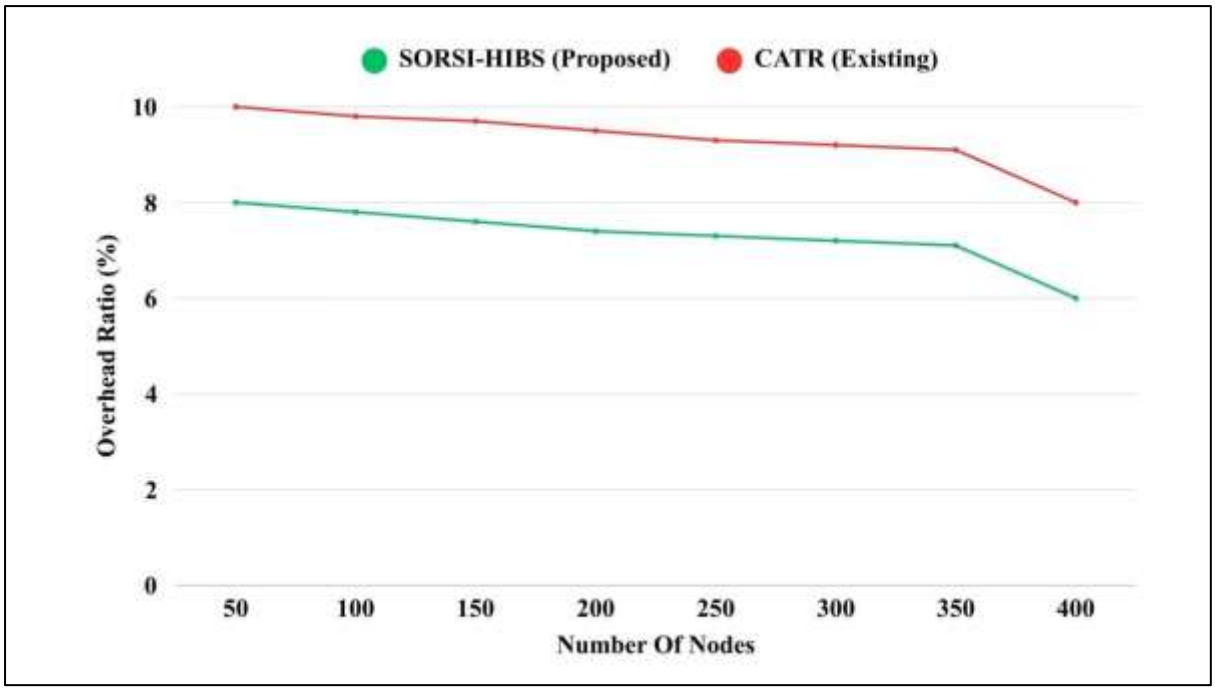

Fig4. 8Number Of Nodes Vs Overhead Ratio (%)

In Table 4.5 and Fig. 4 .5, SORSI-HIBS has lower overhead than CATR at all densities and shows that SORSI-HIBS is an efficient protocol for sending security messages. At the node density of 50, SORSI-HIBS has 8% overhead, with 10% overhead for CATR, which allows SORSI-HIBS to reduce the amount of control messages and duplication of security messages that occur. As the density increases, the advantages of SORSI-HIBS increase. For example, at 400 nodes, the SORSI-HIBS overhead decreases to 6% while the CATR overhead remains higher at 8%. Therefore, the SORSI-HIBS overhead continues to decrease, indicating that it will reduce the additional security message overheads and facilitate an increase in scalability and lessen congestion in dense opportunistic networks.

4.4.2.4 Number of Nodes Vs Average buffer time (s)

Average buffer time is how long the messages are stored in the nodes' buffers before being delivered or forwarded. In the scenario of secure opportunistic networks, the amount of time a message is stored in the node buffers may be longer than average due to delays in verifying the security, the congestion of the network, and a lack of forwarding opportunities. The implementation of the proposed SORSI-HIBS framework allows for faster forwarding of a message by providing priority for the forwarding of a message through trusted and cooperative nodes with sufficient buffer space. When selfish nodes are not allowed to participate in the forwarding of a message, there is a reduced risk that a message will be dropped or delayed due to the unwillingness of a node to forward the message on. Additionally, controlling the replication of messages reduces network congestion on a node-by-node basis and prevents message-buffer overflows. An efficient system for managing buffer time is demonstrated by a lower average buffer time within the secure routing framework as well as a superior level of control over congestion.

Table4. 6 Number of Nodes Vs Average Buffer Time (s)

Number Of Nodes	Average buffer time (s)	
	SORSI-HIBS (Proposed)	CATR (Existing)
50	10.0	24
100	9.8	23
150	8.6	20
200	7.5	18
250	6.3	15
300	5.2	10
350	5.1	9
400	4.0	8

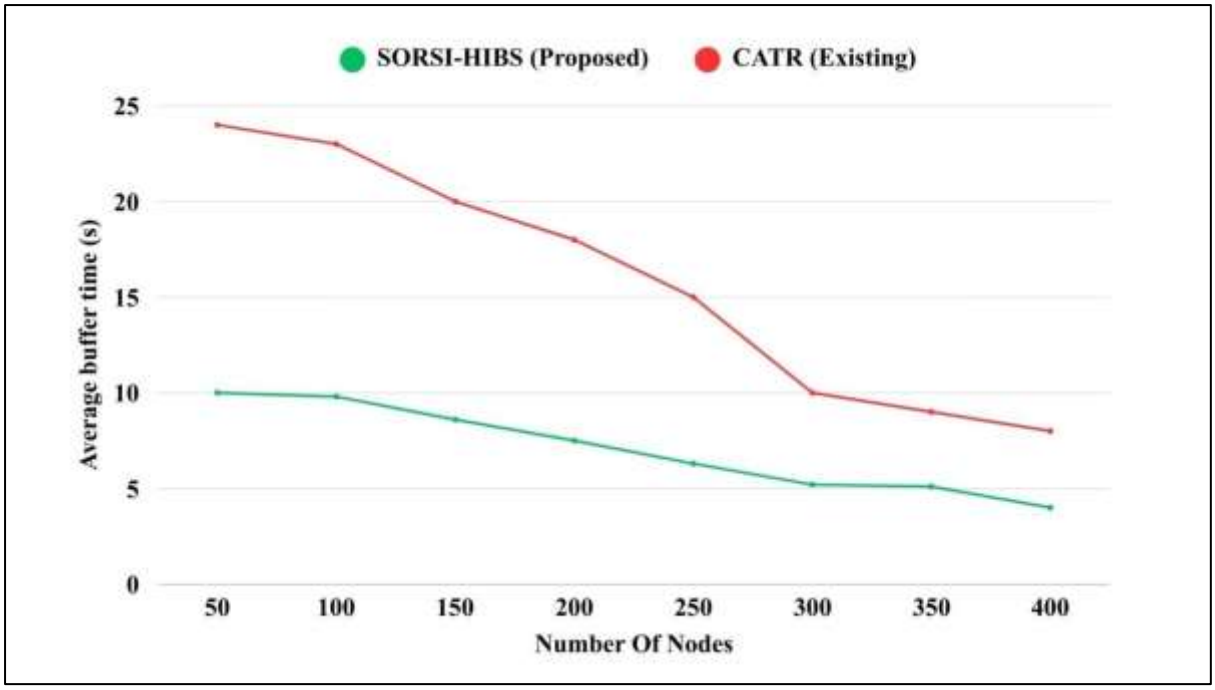

Fig4. 9 Number Of Nodes Vs Average Buffer Time(s)

In Table: 4.6 and Fig. 4 .6, When comparing the proposed SORSI-HIBS protocol to the existing CATR (Current Time and Cost of Routing) protocol, SORSI-HIBS has been proven to reduce the buffer waiting times for packets being sent through the network compared to CATR, allowing for increased efficiency and security when handling packets within networks. In testing a binary tree topology using 50 nodes, the average buffer waiting time using SORSI-HIBS was 10 seconds, while it was found to be 24 seconds using CATR, indicating a significant improvement over CATR's buffering. Compared to SORSI or HIBS, the key difference in the performance of SORSI-HIBS is attributable to the use of lower processing resources,s faster packet transmission ability to provide an envelope around a packet during transmission, as well as secure delivery of the packets. As the number of nodes increases within the network size, SORSI-HIBS's ability to handle packets remains constant, allowing for continued reduced buffering times when compared to CATR. For example, when testing with 400 nodes, SORSI-HIBS further reduced buffer waiting times to an average of four seconds while CATR still had an average buffer waiting time of eight seconds. These results indicate SORSI-HIBS effectively scales with the network density, allowing for minimization of congestion and also allowing for packets to move quickly through the network and remain secure, all while being faster than CATR.

4.4.2.5 Number of Nodes Vs Energy consumption (J)

When assessing secure routing protocols deployed in opportunistic networks, energy consumption is one of the most important indicators of protocol viability because nodes in opportunistic networks use considerable energy when performing all required tasks. As the node count increases, the amount of energy consumed will also incrementally increase because, as each subsequent node performs the activities specified above, they are consuming energy. The secure routing framework provides a means to reduce energy consumption by utilizing lightweight identity-based encryption, in addition to employing a routing architecture that prevents excessive message replication. By only forwarding messages through nodes that are cooperating to forward messages, and by eliminating any potential for redundant retransmissions, the total amount of energy expended during both routing and security operations has been significantly reduced. The energy consumption results are evidence of the proposed security mechanism's energy-efficient capabilities, making it an ideal solution for use in large-scale opportunistic network environments.

Table4. 7 Number of Nodes Vs Energy consumption (J)

Number Of Nodes	Energy consumption (J)	
	SORSI-HIBS (Proposed)	CATR (Existing)
50	2	50
100	10	51
150	20	52
200	35	53
250	40	54
300	45	55
350	50	57
400	58	62

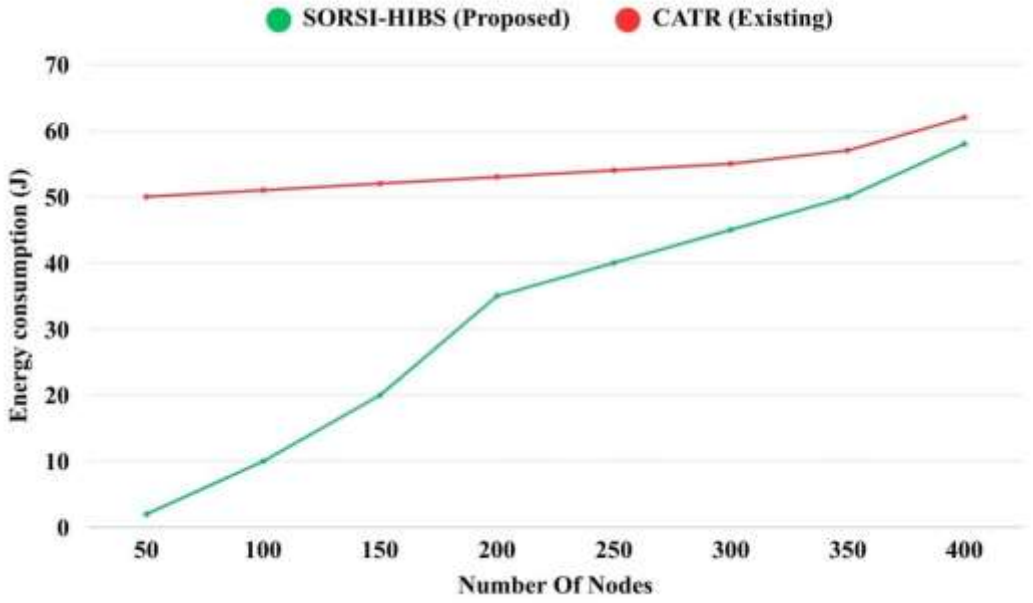

Fig4. 10 Number Of Nodes Vs Energy Consumption (J)

In Table 4.7 and Fig 4.8, Energy consumption rises with the increase in the number of nodes for both the protocols. The amount of energy consumed by SORSI-HIBS is significantly lower than the amount consumed by CATR. For example, SORSI-HIBS uses up only 2 joules when operating with 50 nodes, while CATR uses 50 joules of energy. As for operating with 400 nodes, SORSI-HIBS utilizes 58 joules of energy, and CATR utilizes 62 joules of energy, confirming that the energy-efficient security that we have proposed through our secure

Mechanism is attained. With lower node densities, there is a very clear difference between these protocols in terms of energy efficiency because SORSI-HIB disseminates messages by reducing redundancy and controlling message flooding. As node density increases, the overall energy consumption of both protocols converges on a slightly smaller number, but SORSI-HIB has consistently lower energy consumption than either SORSI-HIB. Therefore, SORSI-HIBS is well-suited to energy-limited opportunistically-based networks, as well as IoT-based applications where extended network lifetime is paramount.

4.5 Results and Discussion

Our proposed SPONS framework for providing security and privacy for opportunistic networks is evaluated using a real-world environment with heterogeneous mobility, intermittent connectivity, and compared to existing protocols, ECSUO and CATR, under the same simulation conditions. The results show that SPONS consistently delivers a higher delivery ratio, lower average latency, and less overhead than ECSUO and CATR. In the early phases of the simulation (2000 seconds), SPONS had a delivery ratio of 55%, compared to ECSUO's delivery ratio of 21% and CATR's delivery ratio of 11%, which indicates that the SPONS design enables faster stabilization of routing paths through its ability to detect and enforce cooperativeness with selfish nodes. Over the duration of the simulation, SPONS experienced an increase in delivery ratio that reached 68% at the conclusion of the simulation, which was 42000 seconds in length. In comparison, ECSUO achieved a delivery ratio of 25% and CATR achieved a delivery ratio of 15%. This shows that SPONS is able to offer a consistently high level of reliability when used within a dynamic network environment. Further evidence of the Efficiency of SPONS can also be seen through the analysis of Latency. At the 500-second Latency mark, SPONS had a cumulative delivery probability of 0.58. This is a larger-than-expected delivery rate when compared to both ECSUO (0.185) and CATR (0.160). Thus, for those messages that were delivered, SPONS delivered significantly more messages in shorter time periods than either ECSUO or CATR was able to do. Even when looking at larger-than-expected Latency levels (in the area of 18,000 seconds), SPONS has a cumulative delivery probability of 0.68, while ECSUO and

CATR both show significant performance loss as Latency increases. The reason for this improvement is due to the following: 1) cooperative node selection; 2) less congested buffers; and 3) probabilistic forwarding based on connection histories. According to the overhead ratio results, SPONS reduces redundant transmissions significantly. At the time interval of 2000 s, the overhead ratio generated by SPONS is 32%, while ECSUO is 50%, and CATR is 60%. The overhead ratio continues to increase over time; however, SPONS maintains an overall overhead ratio that is lower than ECSUO and CATR throughout the duration of the analysis. At 42000 s SPONS has an overall overhead ratio of 52%, ECSUO and CATR. Therefore, SPONS balances reliability, timeliness, and efficiency by utilising a system that allows selfish node detection, provides incentive-based cooperation, and implements identity-based security systems, making it an appropriate choice for a secure, privacy-protecting mobile communication in a dynamic, opportunistic network.

SPONS shows significantly better energy efficiency and improved buffer usage compared to ECSUO and CATR, in addition to its improvements in delivery ratio, latency, and overhead performance. Because the limited storage capacity and intermittent connectivity of such types of networks increase the need for efficient buffer management, it is essential to utilize the SPONS framework and its lower overall average time spent by messages waiting in the node buffer to be forwarded or delivered. The selective forwarding approach followed by SPONS, in which only nodes with sufficient buffer capacity cooperate with relaying and forwarding messages, primarily accounts for these results.

The effectiveness of the proposed framework is demonstrated by energy consumption analysis conducted on mobile opportunistic networks that often contain devices with limited power. Therefore, a fundamental goal of the design of any such network is to enable energy-efficient routing [179]. Because of its reduced number of duplicate transmissions and lightweight security (i.e., identity-based encryption), the SPONS framework results in a lower energy consumption potential than the ECSUO and CATR routing protocols. Becoming less reliant upon extensive efforts in cryptographic processing, the SPONS framework has developed identity-based encryption as a security method and so does not

necessitate extensive computational processing for maintaining data confidentiality whilst providing a level of security. Therefore, devices within the SPONS framework are able to save energy whenever they forward messages or enforce security, thereby enhancing the ability of devices within a network over time to sustain themselves longer with a large number of nodes operating simultaneously [188].

A notable unique feature of SPONS relates to its ability to adapt to selfish node behavior through the use of a dynamic mechanism for detecting selfishness based on the history of actual interactions with the nodes. In doing so, SPONS dynamically evaluates the level of a particular node's cooperation based on the way it has behaved in the past. This means that SPONS is able to quickly identify nodes that do not forward packets and also adaptively exclude those uncooperative nodes from future routing activities. On the other hand, ECSUO, CATR, and similar mechanisms employ methods of evaluating trust in an indirect or delayed fashion; therefore, selfish nodes can continue to operate in the routing environment for a prolonged period of time, thus increasing the likelihood of dropped packet And inefficient routes being formed. As a result, the ability of SPONS to rapidly adapt to changes in node behavior, combined with the reliability of the routing environment, is a significant improvement to the routing reliability of any highly dynamic environment.

Scalability testing found SPONS is consistently effective as network size and node density increase. SPONS also displays stable performance metrics with respect to overhead ratio, delivery success percentage, and latency when compared against rapid declines of ECSUO and CATR performance due to overhead and other impacts of excessive densities. Moreover, the gradual increase of overhead, in addition to high rates of successful delivery and low latencies, provides proof that SPONS has an effective means to handle the unique characteristics of both sparse and dense environments, which will be beneficial to the ongoing deployment of SPONS in real-world scenarios (i.e., disaster recovery efforts, military communications, vehicular networks, mobile social networks, etc.) in which the size of a node's surrounding node population, as well as node population density and mobility patterns, is often variable in both time and space.

SPONS provides an optimal solution to the security, efficiency, and reliability problem of existing opportunistic routing protocols by integrating several independent yet complementary components to form a comprehensive routing framework that provides optimal message delivery, reduces resource consumption, and improves the overall trustworthiness of the network. Networking environments that require secure, privacy-friendly, and efficient communications in dynamic conditions.

4.6 Summary

This project starts off with a Network ONE Simulator platform, which creates a simulation of mobile nodes in a very large OppNet. The OppNet environment was designed to simulate wireless communications as closely as possible to how they would occur in a real wireless network. After creating the network scenario and simulating the execution, we gathered data on several different network parameters, including packet transmission time, packet size, and packet reception count. The next step is to implement message routing performance based on the “SECESW-DSA” messaging system to improve how messages are forwarded by considering high delivery message efficiency, node stability, y and the length of links in a dynamic environment. Further to this, the message communication is secured against misbehaviour and selfish node behaviour using the framework outlined in this paper entitled “SORSI”, and the HIBS algorithm is proposed as a method for increasing the security and authenticity of communication to protect against malicious interference, to promote trust and integrity, and to verify our secure identity within OppNets. In assessing the performance of our proposed model, multiple metrics were created and plotted on a graph with the following three measurements: “Time versus Delivery Ratio”, “Average Latency versus Cumulative Probability”, and “Time versus Overhead Ratio”.

The evaluation results obtained from these performance metrics demonstrate that the proposed integrated framework significantly enhances both routing efficiency and security in opportunistic networks. The method i.e. Stability-Aware Routing Mechanism detects the presence of reliable forwarding paths even in extreme Mobile Network Condition (MNC) due to improved delivery ratios and ability to detect and use Buffered Encounter History (BEH)

to reduce replicates while allowing for a dependable end-to-end communication link when paired with Adaptive Copy Control (ACC) capabilities. Performance delivery and resource utilization balance must be met to be able to deploy large scale Opportunistic Network. Latency analysis results show the effectiveness of the proposed solution. The proposed solution's improved relay node selection methods and reduced buffer congestion have enabled the rapid delivery of messages with lower latency averages than traditional routing and security protocols. The cumulative delivery probability curves indicate that many more messages are delivered in shorter time frames than with traditional routing and security protocols. The improvements of the solution demonstrate that when the stability of the node is taken into account when using cooperative forwarding techniques, messages will experience significantly less delay due to unreliability or selfish behavior of nodes during transmission within opportunistic environments. Using the overhead ratio results, the proposed model is capable of delivering scalable performance and operational efficiency. The system decreases the network's transmission overhead by allowing messages to be delivered only through nodes that offer both cooperative support and the requisite resources. The gradual increase of overhead over time indicates that both routing and security mechanisms remain lightweight, despite increased network activity and longer duration. The network requires this capability to ensure functionality in low-bandwidth and power-constrained environments as well as during times of network disconnection. The SORSI System detects Selfish Nodes and isolates them to ensure that only those users who are trusted are able to send messages and that these messages are sent securely via the Network Security Mechanism. By using this Network Security Mechanism, combined with an Incentian System for co-operation between Nodes, there is a continuous and reliable way for Nodes to work together to form a reliable Network, which in turn, develops a robust and resilient Network. The use of a Hierarchical Identity-Based Security (HIBS) system provides a secure method for transmitting Data by providing a means to maintain Confidentiality and Authentication of Data, along with providing Integrity Checks. HIBS provides a way to perform these actions independently of a Centre rate Certificate Authority System. This Method is advantageous in

a Decentralised Environment, such as Opportunistic Networking, since the Decentralisation provides the opportunity for easier Key Management.

The integration of the SECESW-DSA routing protocol with the SORSI-HIBS Security Framework allows for a complete communication solution with total security while maintaining the operational efficiency of the network. The success of the SECESW-DSA Routing Protocol and the SORSI-HIBS Security Framework is evident in the empirical findings and the results demonstrate that both systems overcome many critical challenges including: routing instability, excess overhead, selfishness of nodes and security vulnerabilities. The information contained within this chapter provides the basis for the concluding analysis and future areas of research that will be outlined in the next chapter which provides a summary of all contributions to the field and provides insights into future research directions.

Chapter 5

This chapter concludes the dissertation by summarizing the contributions and results of the integrated STCESW-DSA routing and SPONS security framework for Opportunistic Networks. Simulation results using the ONE simulator demonstrate significant improvements in routing efficiency, scalability, security, and resource utilization compared to existing approaches. The chapter also outlines the limitations of this work and highlights future research directions, including real-world deployments, cross-layer optimization, AI-assisted routing, and enhanced privacy mechanisms.

The subsequent sections are organized as follows: Section 5.1 presents an overall summary of the results found in the previous chapters, and clearly outlines the rationale behind developing a new framework to improve the effectiveness of the approach; Section 5.2 identifies and describes the primary research contributions made while developing STCESW and SPONS; Section 5.3 summarizes the results of both simulation and comparison analysis; and Section 5.4 presents the future work that will occur based upon these analyses, such as real-world demonstrations of STCESW and SPONS, couplet integrations with other protocols (i.e., application areas), incorporating machine learning technology, and improving the privacy aspects of each.

Conclusion and Future Work

5.1 Conclusion

The purpose of this thesis was to address the major obstacles facing opportunistic networks due to ineffective routing, too much routing overhead due to security concerns, vulnerability to attacks, and lack of scalability. Most of the solutions currently available rely on either flooding-based forwarding or heavy-weight encryption methods, neither of which works well in fast changing environments with very limited resources available. Therefore, a new design framework that uses adaptive routing based on stability awareness combined with cooperation based (i.e., trusting) security methods has been proposed. The STCESW-DSA routing algorithm provides an intelligent way for opportunistic nodes to make forwarding decisions based on contextual information from other nodes within the network. The SORSI-HIBS security framework allows for secure and cooperative message delivery without requiring a central authority. By simulating using The ONE simulator, the findings of this study conclude that the combined design framework provides a significantly higher delivery ratio, lower routing overhead, lower latency, and fewer energy losses than what various existing schemes deliver. Thus, this study demonstrates that stability aware routing with lightweight failures for message delivery and lightweight security can be used effectively in large-scale opportunistic network environments. In conclusion, this research provides a scalable, efficient, and safe manner of conducting opportunistic communications, and can be used to support real-world applications such as disaster recovery, smart cities, and the delay tolerant structure of mobile systems. Apart from enhancing the core routing function, this proposed framework highlights the importance of mutual integration of routing efficiency and security when measured together in contrast to being seen individually. The outcomes of this proposal prove that the integration of stability awareness and cooperation trust evaluation methods into the actual forwarding procedure of a network plays an essential role in boosting network resistance to selfish and malicious behavior from nodes in the network. Thus, the evaluation of the algorithm also confirms that the dynamic adaptability presented in the problem plays an essential role in attaining scalability in Opportunistic Networks. Through the dynamic adaptation of message replication and forwarding mechanisms in accordance with the stability of the network in real-time, the presented STCESW-DSA algorithm alleviates the usual overhead of such approaches in which the factors of replicating messages remain static in nature.

In addition, these findings indicate that providing "Context Awareness" to opportunistic networks is important. It should be noted that because of node stability, contact time, residual energies, buffer presence and Trust, the designed model has Improved Performance according to the different Assessment Criteria. Therefore, by establishing context there is an urgent need for Routing and Security in Opportunistic Environment.

In general, this study offers an initial solution to opportunistic networking by proposing an adaptive, scalable, and secure routing model that addresses issues caused by intermittent connections, high level of mobility, and limited resources. Practically speaking, the combination of stability-aware routing with lightweight secure mechanisms provides the foundation for deployment in the real world. The success of this combined approach highlights the effectiveness of the proposed method and establishes a foundation for researchers to continue to work toward developing intelligent, secure, and efficient means of transmitting messages through next-generation opportunistic networks.

5.2 Research Contribution

This study has provided the following major contributions:

- A collaborative Routing & Security System (R&SS) that provides solutions to Efficiency, Scalability, and Security issues in Opportunistic Networks
- Creation of a Dynamic, Adaptive, Stability- based Spray & Wait routing method (STCESW-DSA) that adjusts to changing network conditions and available resources
- Development of a Resource-Aware Copy Control System that balances Reliability of Delivery with Cost Reduction.
- SORSI improves the trustworthiness and reliability of forwarding messages in a decentralized environment by using selfish nodes to identify faulty nodes.
- While HIBS is an identity-based protocol that provides confidentiality and authentication, it relies on not having to distribute key to anyone through a central authority.
- The study provided an empirical evaluation of various protocols through simulation that highlights significant performance improvements compared to conventional routing and/or security protocols. A Routing Reliability method was developed that combines Stability Awareness, Congestion Control Mechanism, and Trust between Nodes; thus, improving Routing Reliability in Dynamic Environments.
- An opportunity-based Routing method that scales is achieved through the Scalable Control of Message Copies and an Intelligence-Based Selection of Relay Nodes, allowing for maximum reliability when using An Opportunistic Routing method in both Medium and High Density Networks.
- Performance Evaluation has been carried out using Real Life Movement Patterns and a large Simulation Study comparing the New Framework with Current State-of-the-Art Routing/Security Protocols in the Industry.

- Through several unique performance metrics (delivery ratio, overhead ratio, average latency, buffer residence time, and security effectiveness), the quantitative validation of this method is shown to produce acceptable results with respect to the proposed method.
- It demonstrates that the current integrated routing–security co-design can be more effective than either routing or security solutions alone, thereby creating a viable scalable architecture for future opportunistic and delay-tolerant networks.

5.3 Findings

Experimental results have shown that the addition of stability awareness and dynamic adaptability to opportunistic routing produces a marked improvement in network performance. The routing algorithm developed called STCESW-DSA outperforms other community-based methods with respect to delivery ratio especially within the medium to high density range of operation. The increase in delivery ratios can be traced primarily to the ability to make informed decisions regarding forwarding messages through nodes taking into account factors like node mobility, how long they will be in contact with each other, remaining energy levels and how much space they have available in their buffers. The dynamic copy control system minimizes message transmission overhead, enhancing scalability through significantly reduced overhead ratios. The lower overall average buffering delays and lower average latency times indicate that the opportunity for contact (i.e., contact opportunity), as well as the ability to control congestion effectively was maximised. With regard to detecting selfish nodes and promoting cooperative behavior among nodes, the SORSI-HIBS framework meets all of these needs and provides an end-to-end confidentiality solution for data that is transmitted. SORSI employs identity-based encryption (IBE) to replace a centralized key management (CKM) infrastructure, which helps to reduce the amount of overhead associated with cryptography while enabling SORSI's ability to be used in resource-constraint networks.

Based on the experimental results, the addition of dynamic adaptability and stability awareness to opportunistic routing provides considerable and measurable performance benefits to the existing networking systems. The STCESW-DSA routing algorithm provides consistently higher performance than other community-based routing protocols tested in this research for all types of scenarios tested and shows the greatest improvements with the medium-to-high-density network scenarios.

The results obtained from the simulation of the STCESW-DSA route planning algorithm demonstrate a much higher delivery ratio than that achieved with traditional community-based routing schemes, ranging from approximately a 15% improvement at low node density levels to approximately 30% at medium to high node densities. The improvements in delivery ratios experienced with the STCESW-DSA routing algorithm are primarily attributed to the use of reliable forwarding decisions based on informed forwarding decisions that consider node mobility patterns, expected contact times, available energy levels, and available buffer space when selecting relay nodes.

By using a dynamic copy control mechanism to reduce message retransmissions, routing overhead and consequently network resource use has been reduced by 25- 40% through implementation of the Dynamic Copy Control mechanism(s). This implementation has also significantly increased the scalability of network resources available for routing user defined packets, as well as decreased delays in packet transfer from sender to receiver. The reduction in packet retransmissions provides a mechanism for reducing congestion and maintaining an acceptable level of delivery capabilities.

The delay performance of STCESW-DSA is significantly better than baseline routing protocol based on average end-to-end latency of 10-25% lower when compared to baseline routing protocol. Additionally, STCESW-DSA provides for the ability for the efficient use of contact opportunities during the encounter of network nodes based on average buffer residence time (i.e., how long the packet remains within the buffer). By minimizing the buffer residence time of packets, congestion control has been successfully achieved.

In terms of security, and cooperation between nodes, the SORSI-HIBS framework provides for the identification of selfish node behavior and the encouragement of cooperative node behavior within the network. Simulation results show high accuracy of selfish node detection, which translated into a significant increase in the number of successful message deliveries to their respective destinations, resulting from the cooperation of non-selfish nodes. Furthermore, the cooperative enforcement mechanism promotes increased cooperation of trusted nodes in the routing process. With the introduction of identity-based encryption (IBE) into SORSI, there is no longer a need for a centralized key management (CKM) system. By eliminating the CKM system, the implementation of identity-based encryption (IBE) decreases the overhead of using public key based systems, roughly between 20 and 30%, allowing the framework to be more efficient in resource-constrained opportunistic networks while maintaining end-to-end data confidentiality for secure communication without sacrificing routing performance.

In summary, Results from the implementation of the combined STCESW-DSA and SORSI-HIBS framework show that there is a good balance of Delivery Performance, Lower Overhead, Reduced Latency, and High Security, providing evidence to support its effectiveness in implementing Secure and Scalable Opportunistic Networks.

5.4 Future Work

Despite the success of this proposed framework there remain opportunities for additional research and development as outlined below:

- Through practical use, testing on actual devices, and operating under real-world environment (e.g., mobility) conditions to evaluate how they perform based on the devices used and the radio/antenna system.

- Detect behaviour patterns with respect to routing based on information from multiple layers of the protocol stack, including the physical layer and MAC layers, and use this to provide reliability for routing messages.
- Integrate lightweight learning models to provide greater accuracy for predictions of stability and for adaptive forwarding decision making.
- Provide mechanisms that protect user privacy by providing higher levels of anonymity and location-based privacy.
- Anonymity/privacy by implementing sophisticated Private & Geo-encryption of privacy-preserving technology.
- Low overhead requirements for developing/Incentivizing cooperative and trustworthy efforts through use of light-weight Blockchain-enabled incentive strategies.

Practical Application and Testing: In future studies, researchers will expand the Mobile System Validation framework by creating test scenarios on actual mobile devices to verify the performance of the framework in real-world settings such as using multiple and varied hardware types, different radio and antenna types, energy limitations, and realistic mobile movement patterns. Performing these tests will provide researchers with information proving the framework's ability to be scalable, reliable, and viable compared to results from previous simulation tests.

Studying Routing Intelligence across Layers: Understanding cross-layer information (physical layer and the MAC layer) may help Network Engineers create Routing Decisions. The most effective method for using cross-layer information to create Routing Decisions is to use Link Quality, Signal Strength Variation, Channel Contention, and the Reliability of Transmission as factors when routing messages over a highly dynamic network environment. By including these Routing Factors into the Routing Process, Network Engineers will achieve More Stable Routing and a More Reliable Means of Successfully Delivering Messages in Highly Dynamic Network Environments.

Utilizing AI/Machine Learning Techniques for Adaptable Routing: To improve accuracy of forecasting stable nodes in routing protocols, as well as capacity to identify nodes for use in routing packets continues to advance. Current AI & ML techniques need to be developed with very little processing and electrical power for the many operational limits associated with opportunistic networks, IoT devices.

Privacy and Anonymity Technology: Future technology improvements will likely focus on improving the user's ability to be anonymous and to protect their privacy based upon their location. Advanced privacy-preservation technology (e.g., Private Encryption, Geo-Encryption) could be used to protect users' sensitive data while allowing for maximum efficiency in routing.

Incentive and Trust Management using Blockchain Technology: The development of lightweight, blockchain-enabled incentives may stimulate co-operation/trustworthy actions between participating nodes. Decentralized, tamper-free, ledgers could potentially reduce the incentives for selfish behaviour, while at the same time minimising the communication and computational resources used to perform such.

Extensions of the 6G and IoT Network: The proposed framework can be extended to include the support of future communication technologies such as 6G, along with the needs of an expanding range of IoT applications. The needs related to the rapidly growing population who require extremely dense connectivity, low latency, and intelligent network functionality will require additional future research and development for applications in smart cities, cyber-physical systems, and next-gen wireless systems.

Combining Delay-Tolerant Applications with Disaster Recovery: Future research may examine the application of the proposed framework in disaster recovery scenarios and delay-tolerant communication environments. These opportunistic networks are excellent at filling in when regular systems are destroyed or simply fail to function following a disaster. To demonstrate how effectively the Emergency Management Communications system can be used to create the Emergency Management System (EMS), we should extend this framework

to include other applications such as: search & rescue (S&R) operations; emergency notifications; first responders information sharing; and while creating EMS a primary goal will be to implement smart data transmissibility modes with an emphasis placed on resiliency and high-priority messaging. Thus, by providing methods of delivering priority messages before everything else within an EMS, there will be enhanced capability for every participating agency during emergency operations.

Extending Heterogeneous Network Interoperability Framework: to include opportunistically-Connected Nodes in Infrastructure-Based Networks (e.g., Cellular, Satellite, Edge Computing). Seamless interoperability between OppNet and Infrastructure Networks can be achieved through the intelligent use of existing connectivity within Large-Scale IoT Ecosystems, Smart Cities, and Similar Applications.

References

1.Mishra, Sushil Kumar (2024) An Authentication and Privacy Preservation Technique for Opportunistic Network. http://hdl.handle.net/10603/636669

2.Deep Kumar Bangotra (2022) Intelligent and Secure Opportunistic Routing in Wireless Sensor Networks. http://hdl.handle.net/10603/443700

3.Rashidibajgan, S., & Hupperich, T. (2022). Improving the performance of opportunistic networks in real-world applications using machine learning techniques. *Journal of Sensor and Actuator Networks*, *11*(4), 61.

4.Khalil, A., & Zeddini, B. (2024). A Secure Opportunistic Network with Efficient Routing for Enhanced Efficiency and Sustainability. *Future Internet*, *16*(2), 56.

5.Su, B., & Liang, J. (2024). Research on Secure Community Opportunity Network Based on Trust Model. *Future Internet*, *16*(4), 121.

6.Chaurasia, S., & Kumar, K. (2023). MOORP: Metaheuristic based optimized opportunistic routing protocol for wireless sensor network. *Wireless Personal Communications*, *132*(2), 1241-1272.

7.Singh, J., Dhurandher, S. K., Woungang, I., & Chao, H. C. (2024). Context-Aware Trust and Reputation Routing Protocol for Opportunistic IoT Networks. *Sensors*, *24*(23), 7650.

8.Yamamoto, R., Yamazaki, T., & Ohzahata, S. (2023). VORTEX: Network-Driven Opportunistic Routing for Ad Hoc Networks. *Sensors*, *23*(6), 2893.

9.Rashidibajgan, S., & Hupperich, T. (2024). Utilizing blockchains in opportunistic networks for integrity and confidentiality. *Blockchain: Research and Applications*, *5*(1), 100167.

10. Malik, A. (2023). A social relationship-based energy efficient routing scheme for Opportunistic Internet of Things. *ICT Express*, *9*(4), 697-705.

11. Jesús-Azabal, M., García-Alonso, J., Soares, V. N., & Galán-Jiménez, J. (2022). Improving delivery probability in mobile opportunistic networks with social-based routing. *Electronics*, *11*(13), 2084.

12. Khalid, K., Woungang, I., Dhurandher, S. K., Singh, J., & JPC Rodrigues, J. (2020). Energy-efficient check-and-spray geocast routing protocol for opportunistic networks. *Information*, *11*(11), 504.

13. Kazmi, S. H. A., Qamar, F., Hassan, R., & Nisar, K. (2023). Routing-based interference mitigation in SDN enabled beyond 5G communication networks: A comprehensive survey. *IEEe Access*, *11*, 4023-4041.
14. Su, B., & Zhu, B. (2023). TBMOR: A lightweight trust-based model for secure routing of opportunistic networks. *Egyptian Informatics Journal*, *24*(2), 205-214.
15. Xiong, Y., & Jiang, S. (2023). Multi-Decision Dynamic Intelligent Routing Protocol for Delay-Tolerant Networks. *Electronics*, *12*(21), 4528.
16. Li, L., Gou, F., Long, H., He, K., & Wu, J. (2022). Effective data optimization and evaluation based on social communication with AI-assisted in opportunistic social networks. *Wireless Communications and Mobile Computing*, *2022*(1), 4879557.
17. Kluss, B., Rashidibajgan, S., & Hupperich, T. (2022). Blossom: cluster-based routing for preserving privacy in opportunistic networks. *Journal of Sensor and Actuator Networks*, *11*(4), 75.
18. Yu, L., Xu, G., Wang, Z., Zhang, N., & Wei, F. (2022). A hybrid opportunistic IoT secure routing strategy based on node intimacy and trust value. *Security and Communication Networks*, *2022*(1), 6343764.
19. Rajasekar, V., Jayapaul, P., Krishnamoorthi, S., Saracevic, M., Elhoseny, M., & Al-Akaidi, M. (2022). Enhanced WSN routing protocol for Internet of Things to process multimedia big data. *Wireless Personal Communications*, *126*(3), 2081-2100.
20. Han, Y., Hu, H., & Guo, Y. (2022). Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. *IEEe Access*, *10*, 11538-11550.
21. Khan, Z. A., Amjad, S., Ahmed, F., Almasoud, A. M., Imran, M., & Javaid, N. (2023). A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks. *IEEE Access*, *11*, 31036-31051.
22. Gebremariam, G. G., Panda, J., & Indu, S. (2023). Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models. *Alexandria Engineering Journal*, *82*, 82-100.
23. Rimani, J., Mascolo, L., & Fraire, J. A. (2022). A parametric data handling evaluation framework for autonomous lunar networks. *CEAS Space Journal*, *14*(2), 365-376.
24. Domingues, A. C., de Souza Santana, H., Silva, F. A., de Melo, P. O. V., & Loureiro, A. A. (2022). SocialRoute: A low-cost opportunistic routing strategy based on social contacts. *Ad Hoc Networks*, *135*, 102949.

25. de Toro, M., Borrego, C., & Robles, S. (2022). A controller-driven approach for Opportunistic Networking. *Applied Sciences*, *12*(23), 12479.
26. Cao, Y., Li, P., Liang, T., Wu, X., Wang, X., & Cui, Y. (2023). A novel opportunistic network routing method on campus based on the improved Markov model. *Applied Sciences*, *13*(8), 5217.
27. Soelistijanto, B. (2022). Construction of optimal membership functions for a fuzzy routing scheme in opportunistic mobile networks. *IEEE Access*, *10*, 128498-128513.
28. Wang, Z., Jiao, Y., & Wu, J. (2022). User-optimized data transmission scheduling based on edge community service in opportunistic social network. *IET Communications*, *16*(15), 1838-1852.
29. Sharifi Sani, M., Iranmanesh, S., Salarian, H., Tubbal, F., & Raad, R. (2024). Optimizing Energy Efficiency in Opportunistic Networks: A Heuristic Approach to Adaptive Cluster-Based Routing Protocol. *Information*, *15*(5), 283.
30. Hai, T., Zhou, J., Lu, Y., Jawawi, D., Wang, D., Onyema, E. M., & Biamba, C. (2023). *Enhanced security using multiple paths routine scheme in cloud-MANETs, J. Cloud Comput 12 (1): 68*.
31. Wu, J., Dai, T., Guan, P., Chen, Z., Gou, F., & Taherkordi, A. (2025). Opportunistic routing for mobile edge computing: a community detected and task priority aware approach. *Computer Networks*, *258*, 111000.
32. Li, L., Gou, F., & Wu, J. (2022). Modified data delivery strategy based on stochastic block model and community detection in opportunistic social networks. *Wireless Communications and Mobile Computing*, *2022*(1), 5067849.
33. Shu, J., Shi, J., & Liao, L. (2022). F Link prediction model for opportunistic networks based on feature fusion. *IEEE Access*, *10*, 80900-80909.
34. Chen, J., Bie, P., Nie, J., & Wei, Z. (2024). HP-ECD: Heuristic Prophet protocol based on energy balance, cache optimization, and asynchronous dormancy. *Journal of King Saud University-Computer and Information Sciences*, *36*(1), 101861.
35. Li, Q., Zhang, L., Zeng, F., Pan, Y., & Yang, J. (2022). Community clustering routing algorithm based on information entropy in mobile opportunity network. *IEEE Access*, *10*, 25755-25766.
36. Li, P., Cao, Y., Jia, H., Wang, X., & Wu, X. (2025). Congestion Control Method for Campus Opportunity Network Based on Ant Colony Algorithm. *Chinese Journal of Electronics*, *34*(2), 576-585.

37. Ryu, J., & Kim, S. (2023). Reputation-based opportunistic routing protocol using q-learning for manet attacked by malicious nodes. *IEEE Access*, *11*, 47701-47711.
38. Huang, J., Gou, F., & Wu, J. (2023). An effective data communication community establishment scheme in opportunistic networks. *Iet Communications*, *17*(12), 1354-1367.
39. Baumgartner, M., Papaj, J., Kurkina, N., Dobos, L., & Cizmar, A. (2024). Resilient enhancements of routing protocols in MANET. *Peer-to-Peer Networking and Applications*, *17*(5), 3200-3221.
40. Sedjelmaci, H., Kaaniche, N., Boudguiga, A., & Ansari, N. (2023). Secure attack detection framework for hierarchical 6G-enabled internet of vehicles. *IEEE Transactions on Vehicular Technology*, *73*(2), 2633-2642.
41. Wang, J., Liu, Y., Niu, S., & Song, H. (2021). Lightweight blockchain assisted secure routing of swarm UAS networking. *Computer Communications*, *165*, 131-140.
42. Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Al Hamadi, H. (2022). Private blockchain-based encryption framework using computational intelligence approach. *Egyptian Informatics Journal*, *23*(4), 69-75.
43. Panahi, U., & Bayılmış, C. (2023). Enabling secure data transmission for wireless sensor networks based IoT applications. *Ain Shams Engineering Journal*, *14*(2), 101866.
44. Tilwari, V., Maheswar, R., Jayarajan, P., Sundararajan, T. V. P., Hindia, M. N., Dimyati, K., ... & Amiri, I. S. (2020). MCLMR: A multicriteria based multipath routing in the mobile ad hoc networks. *Wireless Personal Communications*, *112*(4), 2461-2483.
45. Yang, L., Lu, Y., Yang, S. X., Guo, T., & Liang, Z. (2020). A secure clustering protocol with fuzzy trust evaluation and outlier detection for industrial wireless sensor networks. *IEEE Transactions on Industrial Informatics*, *17*(7), 4837-4847.
46. Javaid, N. (2022). A secure and efficient trust model for wireless sensor IoTs using blockchain. *IEEE Access*, *10*, 4568-4579.
47. Elisa, N., Yang, L., Chao, F., Naik, N., & Boongoen, T. (2023). A secure and privacy-preserving e-government framework using blockchain and artificial immunity. *Ieee Access*, *11*, 8773-8789.
48. Fan, Y., Zhao, G., Lei, X., Liang, W., Li, K. C., Choo, K. K. R., & Zhu, C. (2021). SBBS: A secure blockchain-based scheme for IoT data credibility in fog environment. *IEEE Internet of Things Journal*, *8*(11), 9268-9277.
49. Wu, C., Ju, B., Wu, Y., Xiong, N. N., & Zhang, S. (2020). WGAN-E: A generative adversarial networks for facial feature security. *Electronics*, *9*(3), 486.

50. Zhang, X., Li, Y., Xiong, Z., Liu, Y., Wang, S., & Hou, D. (2024). A resource-based dynamic pricing and forced forwarding incentive algorithm in socially aware networking. *Electronics*, *13*(15), 3044.
51. Hellaoui, H., Koudil, M., & Bouabdallah, A. (2020). Energy efficiency in security of 5G-based IoT: An end-to-end adaptive approach. *IEEE Internet of Things Journal*, *7*(7), 6589-6602.
52. Narayana, P., Keerthi, K., Khalaf, O. I., Chithaluru, P., Patil, M. A., Tumula, S., ... & Sharif, M. S. (2024). Energy-efficient and secure routing strategy for opportunistic data transmission in WSNs. *Journal of Cyber Security Technology*, 1-36.
53. Hassan, S. M., Mohamad, M. M., Muchtar, F. B., & Dawoodi, F. B. Y. P. (2024). Enhancing MANET Security through Federated Learning and Multiobjective optimization: A Trust-aware Routing Framework. *IEEE Access*.
54. Ma, H., Wu, H., Xing, L., Xie, P., & Wang, D. (2021). VideoOR: a quality oriented replication scheme for video opportunistic transmission. *Wireless Personal Communications*, *118*(4), 2941-2963.
55. Bharathi, R., Kannadhasan, S., Padminidevi, B., Maharajan, M. S., Nagarajan, R., & Tonmoy, M. M. (2022). Predictive model techniques with energy efficiency for IOT-based data transmission in wireless sensor networks. *Journal of sensors*, *2022*(1), 3434646.
56. Elsayed, R., Hamada, R., Hammoudeh, M., Abdalla, M., & Elsaid, S. A. (2022). A hierarchical deep learning-based intrusion detection architecture for clustered internet of things. *Journal of Sensor and Actuator Networks*, *12*(1), 3.
57. Haseeb, K., Almustafa, K. M., Jan, Z., Saba, T., & Tariq, U. (2020). Secure and energy-aware heuristic routing protocol for wireless sensor network. *IEEE Access*, *8*, 163962-163974.
58. Khah, M. A. M., Moghim, N., Gholami, N., & Shetty, S. (2023). Energy-efficient multi-rate opportunistic routing in wireless mesh networks. *IEEE Access*, *11*, 97466-97477.
59. Mohammed, M. H. (2022). An enhancement of cyber security management for opportunistic systems. *Measurement: Sensors*, *24*, 100547.
60. Ramasamy, L. K., Khan, F., Shah, M., Prasad, B. V. V. S., Iwendi, C., & Biamba, C. (2022). Secure smart wearable computing through artificial intelligence-enabled internet of things and cyber-physical systems for health monitoring. *Sensors*, *22*(3), 1076.

61. Pramitarini, Y., Perdana, R. H. Y., Tran, T. N., Shim, K., & An, B. (2022). A hybrid price auction-based secure routing protocol using advanced speed and cosine similarity-based clustering against sinkhole attack in VANETs. *Sensors*, *22*(15), 5811.
62. Saideh, M., Jamont, J. P., & Vercouter, L. (2024). Opportunistic sensor-based authentication factors in and for the internet of things. *Sensors*, *24*(14), 4621.
63. Jeyaselvi, M., Sathya, M., Suchitra, S., Jafar Ali Ibrahim, S., & Kalyan Chakravarthy, N. S. (2022). SVM-based cloning and jamming attack detection in IoT sensor networks. In *Advances in information communication technology and computing: proceedings of AICTC 2021* (pp. 461-471). Singapore: Springer Nature Singapore.
64. Jiao, Z., Zhang, B., Zhang, L., Liu, M., Gong, W., & Li, C. (2020). A blockchain-based computing architecture for mobile ad hoc cloud. *IEEE Network*, *34*(4), 140-149.
65. Chen, Y., Li, R., Zhao, Z., & Zhang, H. (2020). On the capacity of fractal D2D social networks with hierarchical communications. *IEEE Transactions on Mobile Computing*, *20*(6), 2254-2268.
66. Mir, M. Y., Zhu, H., & Hu, C. L. (2022). Enhanced Geographic Routing with One-and Two-Hop Movement Information in Opportunistic Ad Hoc Networks. *Future Internet*, *14*(7), 214.
67. Wu, H., Sang, Q., Wang, Y., Ma, H., & Xing, L. (2021). Copy Adaptive Routing Algorithm Based on Network Connectivity in Flying Ad Hoc Networks. *Mobile Information Systems*, *2021*(1), 8580795.
68. Zhou, H., Wu, T., Chen, X., He, S., & Wu, J. (2021). RAIM: A reverse auction-based incentive mechanism for mobile data offloading through opportunistic mobile networks. *IEEE Transactions on Network Science and Engineering*, *9*(6), 3909-3921.
69. Qiao, L. (2020). Mobile data traffic offloading through opportunistic vehicular communications. *Wireless Communications and Mobile Computing*, *2020*(1), 3093581.
70. Zhong, X., Li, L., Zhang, Y., Zhang, B., Zhang, W., & Yang, T. (2020). Oodt: obstacle aware opportunistic data transmission for cognitive radio ad hoc networks. *IEEE Transactions on Communications*, *68*(6), 3654-3666.
71. Papadopoulos, P., Coit, D. W., & Aziz Ezzat, A. (2024). STOCHOS: Stochastic opportunistic maintenance scheduling for offshore wind farms. *Iise Transactions*, *56*(1), 1-15.
72. Pahlavan, K., & Krishnamurthy, P. (2021). Evolution and impact of Wi-Fi technology and applications: A historical perspective. *International Journal of Wireless Information Networks*, *28*(1), 3-19.

73. Lu, Y., He, R., Chen, X., Lin, B., & Yu, C. (2020). Energy-efficient depth-based opportunistic routing with Q-learning for underwater wireless sensor networks. *Sensors*, *20*(4), 1025.
74. Yu, Y., Yu, J., Chen, Z., Wu, J., & Yan, Y. (2020). A Comprehensive Multi-Scenario Routing Algorithm Based on Fuzzy Control Theory in Opportunistic Social Network. *Symmetry*, *12*(4), 589.
75. Chen, Y. L., Wang, N. C., Liu, Y. S., & Ko, C. Y. (2023). Energy efficiency of mobile devices using fuzzy logic control by exponential weight with priority-based rate control in multi-radio opportunistic networks. *Electronics*, *12*(13), 2863.
76. Mumin, D., Shi, L. L., Liu, L., & Panneerselvam, J. (2020). Data-driven diffusion recommendation in online social networks for the internet of people. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(1), 166-178.
77. Ye, M., Zhou, Z., Zhu, L., Huang, F., Li, T., Wang, D., ... & He, Y. (2024). Improving Transmission in Integrated Unmanned Aerial Vehicle–Intelligent Connected Vehicle Networks with Selfish Nodes Using Opportunistic Approaches. *Drones*, *9*(1), 12.
78. Bangotra, D. K., Singh, Y., Selwal, A., Kumar, N., Singh, P. K., & Hong, W. C. (2020). An intelligent opportunistic routing algorithm for wireless sensor networks and its application towards e-healthcare. *Sensors*, *20*(14), 3887.
79. Islam, M. A., Iqbal, M. A., Aleem, M., Halim, Z., Srivastava, G., & Lin, J. C. W. (2021). Evaluation of Congestion Aware Social Metrics for Centrality-Based Routing. *Wireless Communications and Mobile Computing*, *2021*(1), 5581259.
80. Zhang, Q., Song, Y., Sun, B., & Dai, Z. (2020). Design of routing protocol for opportunistic network based on adaptive motion. *IEEE Access*, *8*, 18228-18239.
81. Papapetrou, E., & Likas, A. (2022). A replication strategy for mobile opportunistic networks based on utility clustering. *Ad Hoc Networks*, *125*, 102738.
82. Li, Z., Chen, Z., Wu, J., & Liu, K. (2020). Routing algorithm based on triangular fuzzy layer model and multi-layer clustering for opportunistic network. *IET Communications*, *14*(17), 2905-2914.
83. Koumaras, H., Makropoulos, G., Batistatos, M., Kolometsos, S., Gogos, A., Xilouris, G., ... & Kourtis, M. A. (2021). 5G-enabled UAVs with command and control software component at the edge for supporting energy efficient opportunistic networks. *Energies*, *14*(5), 1480.

84. Bacanli, S. S., & Turgut, D. (2020). Energy-efficient unmanned aerial vehicle scanning approach with node clustering in opportunistic networks. *Computer Communications*, *161*, 76-85.
85. Kang, M. W., & Chung, Y. W. (2020). An improved hybrid routing protocol combining MANET and DTN. *Electronics*, *9*(3), 439.
86. Salih, Q. M., Rahman, M. A., Asyhari, A. T., Naeem, M. K., Patwary, M., Alturki, R., & Ikram, M. A. (2023). Dynamic channel estimation-aware routing protocol in mobile cognitive radio networks for smart IIoT applications. *Digital Communications and Networks*, *9*(2), 367-382.
87. Islam, N., Altamimi, M., Haseeb, K., & Siraj, M. (2021). Secure and sustainable predictive framework for IoT-based multimedia services using machine learning. *Sustainability*, *13*(23), 13128.
88. Rathee, G., Sandhu, R., Saini, H., Sivaram, M., & Dhasarathan, V. (2020). A trust computed framework for IoT devices and fog computing environment. *Wireless Networks*, *26*(4), 2339-2351.
89. Yilmaz, S., & Dener, M. (2024). Security with wireless sensor networks in smart grids: A review. *Symmetry*, *16*(10), 1295.
90. Srivastava, G., Agrawal, R., Singh, K., Tripathi, R., & Naik, K. (2020). A hierarchical identity-based security for delay tolerant networks using lattice-based cryptography. *Peer-to-Peer Networking and Applications*, *13*(1), 348-367.
91. Zhao, Y., & Srivastava, G. (2021). A wireless mesh opportunistic network routing algorithm based on trust relationships. *IEEE Access*, *10*, 4786-4793.
92. Feng, R., Jiang, S., & Zheng, Z. (2022). Capacity Analysis of Incentive Schemes in Opportunistic Networks. *Journal of Marine Science and Engineering*, *10*(10), 1474.
93. Kyung, Y., Kim, E., & Song, T. (2024). Opportunistic offloading scheme for content delivery service using electro-mobility networks. *IET intelligent transport systems*, *18*(4), 591-598.
94. Tu, J., Tian, D., & Wang, Y. (2021). An active-routing authentication scheme in MANET. *IEEE Access*, *9*, 34276-34286.
95. Luo, H., Wu, Y., Sun, G., Yu, H., & Guizani, M. (2024). ESCM: An efficient and secure communication mechanism for UAV networks. *IEEE Transactions on Network and Service Management*, *21*(3), 3124-3139.
96. Lenando, H., Kurd Ali, A. H., Chaoui, S., & Alrfaay, M. (2021). Innovative mutual information-based weighting scheme in stateless opportunistic networks.

97. Jesús-Azabal, M., García-Alonso, J., & Galán-Jiménez, J. (2024). Evaluating the quality of service of Opportunistic Mobile Ad Hoc Network routing algorithms on real devices: A software-driven approach. *Ad Hoc Networks*, *163*, 103591.

98. Javet, L., Anciaux, N., Bouganim, L., & Pucheral, P. (2025). Edgelet computing: enabling privacy-preserving decentralized data processing at the network edge. *Personal and Ubiquitous Computing*, *29*(1), 45-75.

99. Esiefarienrhe, B. M., Phakathi, T., & Lugayizi, F. (2022, June). Node-based QoS-aware security framework for sinkhole attacks in mobile ad-hoc networks. In *Telecom* (Vol. 3, No. 3, pp. 407-432). MDPI.

100. Niebla-Montero, Á., Froiz-Míguez, I., Fraga-Lamas, P., & Fernández-Caramés, T. M. (2022). Practical latency analysis of a Bluetooth 5 decentralized IoT opportunistic edge computing system for low-cost SBCs. *Sensors*, *22*(21), 8360.

101. Chen, D., Navarro-Arribas, G., Pérez-Solà, C., & Borrell, J. (2023). Message anonymity on predictable opportunistic networks. *Journal of Ambient Intelligence and Humanized Computing*, *14*(11), 15059-15072.

102. Memon, A., Iftikhar, A., Ali, M. N., & Kim, B. S. (2025, August). Enhancing QoS in Opportunistic Networks Through Direct Communication for Dynamic Routing Challenges. In *Telecom* (Vol. 6, No. 3, p. 55). MDPI.

103. Xu, G., Wang, X., Zhang, N., Wang, Z., Yu, L., & He, L. (2021). A routing algorithm for the sparse opportunistic networks based on node intimacy. *Wireless Communications and Mobile Computing*, *2021*(1), 6666211.

104. Devi, G. R., Das, M. S., & Murthy, M. R. (2023). Secure cross-layer routing protocol with authentication key management scheme for manets. *Measurement: Sensors*, *29*, 100869.

105. Dener, M., & Orman, A. (2023). BBAP-WSN: A new blockchain-based authentication protocol for wireless sensor networks. *Applied Sciences*, *13*(3), 1526.

106. Alshehri, A., Badawy, A. H. A., & Huang, H. (2020). FQ-AGO: fuzzy logic Q-learning based asymmetric link aware and geographic opportunistic routing scheme for MANETs. *Electronics*, *9*(4), 576.

107. Qafzezi, E., Bylykbashi, K., Higashi, S., Ampririt, P., Matsuo, K., & Barolli, L. (2025). An intelligent fuzzy-based routing protocol for vehicular opportunistic networks. *Information*, *16*(1), 52.

108. Xu, Y., Liu, J., Shen, Y., Liu, J., Jiang, X., & Taleb, T. (2020). Incentive jamming-based secure routing in decentralized internet of things. *IEEE Internet of Things Journal*, *8*(4), 3000-3013.

109. Shafi, S., Mounika, S., & Velliangiri, S. J. P. C. S. (2023). Machine learning and trust based AODV routing protocol to mitigate flooding and blackhole attacks in MANET. *Procedia Computer Science*, *218*, 2309-2318.

110. Al-Essa, R. I., & Al-Suhail, G. A. (2023). AFB-GPSR: Adaptive beaconing strategy based on fuzzy logic scheme for geographical routing in a mobile ad hoc network (MANET). *Computation*, *11*(9), 174.

111. Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, *110*(4), 1637-1658.

112. Al-Zahrani, F. A. (2020). On modeling optimizations and enhancing routing protocols for wireless multihop networks. *IEEE Access*, *8*, 68953-68973.

113. Jesús-Azabal, M., Herrera, J. L., Laso, S., & Galán-Jiménez, J. (2021). OPPNets and rural areas: an opportunistic solution for remote communications. *Wireless Communications and Mobile Computing*, *2021*(1), 8883501.

114. Banerjee, I., Warnier, M., & Brazier, F. M. (2020). Self-organizing topology for energy-efficient ad-hoc communication networks of mobile devices. *Complex Adaptive Systems Modeling*, *8*(1), 7.

115. Ali, A., Tariq, S., Iqbal, M., Feng, L., Raza, I., Siddiqi, M. H., & Bashir, A. K. (2020). Adaptive bitrate video transmission over cognitive radio networks using cross layer routing approach. *IEEE Transactions on Cognitive Communications and Networking*, *6*(3), 935-945.

116. Nemati, M., Al Homssi, B., Krishnan, S., Park, J., Loke, S. W., & Choi, J. (2022). Non-terrestrial networks with UAVs: A projection on flying ad-hoc networks. *Drones*, *6*(11), 334.

117. Kabaou, M. O., Nesrine, Z., Hassen, H., & Fatma, B. (2023). Performance evaluation of opportunistic schedulers based on fairness and throughput in new-generation mobile networks. *The Journal of Supercomputing*, *79*(16), 18053-18088.

118. Azzoug, Y., Boukra, A., & Soares, V. N. (2020). A probabilistic VDTN routing scheme based on hybrid swarm-based approach. *Future Internet*, *12*(11), 192.

119. Wu, J., Zou, W., & Long, H. (2021). Effective path prediction and data transmission in opportunistic social networks. *IET Communications*, *15*(17), 2202-2211.

120. Singha, S., Jana, B., Jana, S. H., & Mandal, N. K. (2020). A survey to analyse routing algorithms for opportunistic network. *Procedia Computer Science*, *171*, 2501-2511.

121. Yu, Y., Yu, J., Chen, Z., Wu, J., & Yan, Y. (2021). A universal routing algorithm based on intuitionistic fuzzy multi-attribute decision-making in opportunistic social networks. *Symmetry*, *13*(4), 664.

122. Li, L., Wang, H., Liu, Z., & Ye, H. (2020). GIR: an opportunistic network routing algorithm based on game theory. *IEEE Access*, *8*, 201158-201172.

123. Deng, Y., Gou, F., & Wu, J. (2021). Hybrid data transmission scheme based on source node centrality and community reconstruction in opportunistic social networks. *Peer-to-Peer Networking and Applications*, *14*(6), 3460-3472.

124. Freire, D., Borrego, C., & Robles, S. (2022). Corpus for development of routing algorithms in opportunistic networks. *Applied Sciences*, *12*(18), 9240.

125. Wang, J., Dan, W., Li, H., Yan, L., Mei, A., & Tang, X. (2025). Social-Aware Link Reliability Prediction Model Based Minimum Delay Routing for CR-VANETs. *Electronics*, *14*(3), 627.

126. Wu, J., Chen, Z., & Zhao, M. (2020). An efficient data packet iteration and transmission algorithm in opportunistic social networks. *Journal of Ambient Intelligence and Humanized Computing*, *11*(8), 3141-3153.

127. Majeed, D. M., Zhang, L., & Shi, K. (2020). Optimal data collection for mobile crowdsensing over integrated cellular and opportunistic networks. *IEEE Access*, *8*, 157270-157283.

128. Xiong, W., Chen, H., Jiao, Y., Yang, M., Zhou, X., & Wu, J. (2022). A user cache management and cooperative transmission mechanism based on edge community computing in opportunistic social networks. *IET Communications*, *16*(17), 2045-2058.

129. Kumar, A., Singh, K., & Khan, T. (2021). L-RTAM: Logarithm based reliable trust assessment model for WBSNs. *Journal of Discrete Mathematical Sciences and Cryptography*, *24*(6), 1701-1716.

130. Santos, G., Soares, D., Carvalho, C., & Mota, E. (2021). An energy-saving forwarding mechanism based on clustering for opportunistic networks. *Sensors*, *21*(22), 7427.

131. Visca, J., & Baliosian, J. (2022). rl4dtn: Q-learning for opportunistic networks. *Future Internet*, *14*(12), 348.

132. Chen, D., Borrego, C., & Navarro-Arribas, G. (2020). A privacy-preserving routing protocol using mix networks in opportunistic networks. *Electronics*, *9*(11), 1754.

133. Wang, K., Feng, G., Zhang, L., & Wu, J. (2020). Energy transmission and Equilibrium scheme in data communication Opportunistic networks. *Applied System Innovation*, *3*(4), 54.

134. Le Sommer, N., Mahéo, Y., & Baklouti, F. (2020). Multi-strategy dynamic service composition in opportunistic networks. *Information*, *11*(4), 180.

135. Usman, Q., Chughtai, O., Nawaz, N., Kaleem, Z., Khaliq, K. A., & Nguyen, L. D. (2021). A reliable link-adaptive position-based routing protocol for flying ad hoc network. *Mobile Networks and Applications*, *26*(4), 1801-1820.

136. Long, H., Hao, J., Zhang, S., Zhang, Y., & Zhang, L. (2024). Community-based task assignment method in mobile crowd sensing. *IEEE Access*, *12*, 84387-84400.

137. Kang, M. W., Seo, D. Y., & Chung, Y. W. (2020). An efficient delay tolerant networks routing protocol for information-centric networking. *Electronics*, *9*(5), 839.

138. Wang, W., Bai, Y., Feng, P., Huang, J., Sha, M., & Tantai, J. (2021). DTN-balance: a forwarding-capacity and forwarding-queue aware routing for self-organizing DTNs. *Wireless Personal Communications*, *118*(1), 575-598.

139. Koukis, G., Safouri, K., & Tsaoussidis, V. (2024). All about Delay-Tolerant Networking (DTN) contributions to future internet. *Future Internet*, *16*(4), 129.

140. Flores, H. (2024). Opportunistic multi-drone networks: Filling the spatiotemporal holes of collaborative and distributed applications. *IEEE Internet of Things Magazine*, *7*(2), 94-100.

141. Lata, A. A., Kang, M., & Shin, S. (2025). FCM-OR: A local density-aware opportunistic routing protocol for energy-efficient wireless sensor networks. *Electronics*, *14*(9), 1841.

142. Wu, J., Gou, F., Xiong, W., & Zhou, X. (2021). A reputation value-based task-sharing strategy in opportunistic complex social networks. *Complexity*, *2021*(1), 8554351.

143. Chen, S., Chen, Z., Wu, J., & Liu, K. (2020). An adaptive delay-tolerant routing algorithm for data transmission in opportunistic social networks. *Electronics*, *9*(11), 1915.

144. Wu, X., Chang, L., Luo, J., & Wu, J. (2021). Efficient edge cache collaboration transmission strategy of opportunistic social network in trusted community. *Ieee Access*, *9*, 51772-51783.

145. Wu, J., Yin, S., Xiao, Y., & Yu, G. (2020). Effective data selection and management method based on dynamic regulation in opportunistic social networks. *Electronics*, *9*(8), 1271.

146. Martín-Pascual, M. Á., & Andreu-Sánchez, C. (2023). Practical application of mesh opportunistic networks. *Applied System Innovation*, *6*(3), 60.

147. Li, J., He, X. Y., Zhao, D., Yang, G. S., He, D. J., & Chan, S. (2020). Delay-aware and cost-efficient probabilistic transmission for opportunistic networks. *Iet Networks*, *9*(6), 372-377.

148. Celik, A., Saeed, N., Shihada, B., Al-Naffouri, T. Y., & Alouini, M. S. (2021). Opportunistic routing for opto-acoustic internet of underwater things. *IEEE Internet of Things Journal*, *9*(3), 2165-2179.

149. Minhas, H. I., Ahmad, R., Ahmed, W., Waheed, M., Alam, M. M., & Gul, S. T. (2021). A reinforcement learning routing protocol for UAV aided public safety networks. *Sensors*, *21*(12), 4121.

150. Chehbour, F., Doukha, Z., Moussaoui, S., & Guerroumi, M. (2020). OMS: Opportunistic mules for short latency data collection in smart cities. *International Journal of Communication Systems*, *33*(10), e4207.

151. Tsilomitrou, O., & Tzes, A. (2021). Mobile data-mule optimal path planning for wireless sensor networks. *Applied Sciences*, *12*(1), 247.

152. Memon, A., Islam, S. M., Ali, M. N., & Kim, B. S. (2025). Enhancing Energy Efficiency of Sensors and Communication Devices in Opportunistic Networks Through Human Mobility Interaction Prediction. *Sensors*, *25*(5), 1414.

153. Krentz, K. F., & Voigt, T. (2024). Secure opportunistic routing in 2-hop IEEE 802.15. 4 networks with SMOR. *Computer Communications*, *217*, 57-69.

154. Rani, S., Koundal, D., Kavita, F., Ijaz, M. F., Elhoseny, M., & Alghamdi, M. I. (2021). An optimized framework for WSN routing in the context of industry 4.0. *Sensors*, *21*(19), 6474.

155. Chan, L., Gomez Chavez, K., Rudolph, H., & Hourani, A. (2020). Hierarchical routing protocols for wireless sensor network: a compressive survey. *Wireless Networks*, *26*(5), 3291-3314.

156. Sami Oubbati, O., Chaib, N., Lakas, A., Bitam, S., & Lorenz, P. (2020). U2RV: UAV-assisted reactive routing protocol for VANETs. *International Journal of Communication Systems*, *33*(10), e4104.

157. Huang, F., Cui, J., Chang, Y., Wang, T., Wang, M., & Yang, Y. (2024). An Improved Spray and Wait Routing Algorithm Based on Stable Transmission Capacity Evaluation of Nodes in Opportunistic Network. *International Journal of Distributed Sensor Networks*, *2024*(1), 7471329.

158. Hussain, K., Xia, Y., Onaizah, A., & Manzoor, T. (2024). Multi-disjoint path opportunistic networks with hidden Markov Chain modeling. *Alexandria Engineering Journal*, *107*, 47-60.

159. Bakiras, S., Troja, E., Xu, X., & Naves, J. F. (2020). Secure and anonymous communications over delay tolerant networks. *IEEE Access*, *8*, 88158-88169.

160. Mao, Y., Zhou, C., Qi, J., & Zhu, X. (2020). A fair credit-based incentive mechanism for routing in DTN-based sensor network with nodes' selfishness. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 232.

161. Zhang, M., Dong, C., Feng, S., Guan, X., Chen, H., & Wu, Q. (2022). Adaptive 3D routing protocol for flying ad hoc networks based on prediction-driven Q-learning. *China Communications*, *19*(5), 302-317.

162. Wu, J., Jin, H., Cai, S., & Liu, L. (2023). A delay tolerant network routing algorithm based on multi-step double Q-learning. *IET Communications*, *17*(11), 1321-1333.

163. Sharma, D. K., Gupta, S., Malik, S., & Kumar, R. (2020). Latency-aware reinforced routing for opportunistic networks. *IET Communications*, *14*(17), 2981-2989.

164. Li, N., Yan, J., Zhang, Z., Martínez-Ortega, J. F., & Yuan, X. (2021). Geographical and topology control-based opportunistic routing for ad hoc networks. *IEEE Sensors Journal*, *21*(6), 8691-8704.

165. Sai, A. M. V. V., & Li, Y. (2020). A survey on privacy issues in mobile social networks. *IEEE Access*, *8*, 130906-130921.

166. Rehman, G. U., Ghani, A., Zubair, M., Saeed, M. I., & Singh, D. (2023). SOS: Socially omitting selfishness in IoT for smart and connected communities. *International Journal of Communication Systems*, *36*(1), e4455.

167. Graffi, K., & Masinde, N. (2021). LibreSocial: A peer-to-peer framework for online social networks. *Concurrency and Computation: Practice and Experience*, *33*(8), e6150.

168. Eissfeldt, H. (2020). Sustainable urban air mobility supported with participatory noise sensing. *Sustainability*, *12*(8), 3320.

169. Xian, J., Wu, H., Mei, X., Chen, X., & Yang, Y. (2022). Low-delay and energy-efficient opportunistic routing for maritime search and rescue wireless sensor networks. *Remote Sensing*, *14*(20), 5178.

170. Raverta, F. D., Fraire, J. A., Madoery, P. G., Demasi, R. A., Finochietto, J. M., & D'argenio, P. R. (2021). Routing in delay-tolerant networks under uncertain contact plans. *Ad Hoc Networks*, *123*, 102663.

171. Srinidhi, N. N., Sagar, C. S., Deepak Chethan, S., Shreyas, J., & Dilip Kumar, S. M. (2020). An improved PRoPHET-Random forest based optimized multi-copy routing for opportunistic IoT networks. *Internet of Things*, *11*, 100203.

172. Galarza, C. E., Palma, J. M., Morais, C. F., Utria, J., Carvalho, L. P., Bustos, D., & Oliveira, R. C. (2021). A novel theoretical probabilistic model for opportunistic routing with applications in energy consumption for WSNs. *Sensors*, *21*(23), 8058.

173. Mallorquí, A., Zaballos, A., & Briones, A. (2021). DTN trustworthiness for permafrost telemetry IoT network. *Remote Sensing*, *13*(22), 4493.

174. Yao, X. W., Chen, Y. W., Wu, Y., Zhao, K., & Jornet, J. M. (2022). FGOR: Flow-guided opportunistic routing for intrabody nanonetworks. *IEEE Internet of Things Journal*, *9*(21), 21765-21776.

175. Serhani, A., Naja, N., & Jamali, A. (2020). AQ-Routing: mobility-, stability-aware adaptive routing protocol for data routing in MANET–IoT systems. *Cluster Computing*, *23*(1), 13-27.

176. Goudar, G., & Batabyal, S. (2020). Point of congestion in large buffer mobile opportunistic networks. *IEEE Communications Letters*, *24*(7), 1586-1590.

177. Bu, T., Yuan, M., Ji, X., & Qiu, Y. (2025, August). Energy-Partitioned Routing Protocol Based on Advancement Function for Underwater Optical Wireless Sensor Networks. In *Photonics* (Vol. 12, No. 9, p. 878). MDPI.

178. Singh, S., Prasad, D., Rani, S., Singh, A., Alharithi, F. S., & Almotiri, J. (2022). Wireless body area routing protocols impact analysis on entity mobility models with static sink node. *Applied Sciences*, *12*(11), 5655.

179. Malyadri, N., M, R., Nandalike, R., Chavan, P., S, S., P, D., & S, R. (2025). A predictive energy-efficient adaptive routing methodology for Mobile Ad hoc Networks. *IET Networks*, *14*(1), e70001.

180. Prasad, R. (2022). Enhanced energy efficient secure routing protocol for mobile ad-hoc network. *Global Transitions Proceedings*, *3*(2), 412-423.

181. Sirmollo, C. Z., & Bitew, M. A. (2021). Mobility-Aware Routing Algorithm for Mobile Ad Hoc Networks. *Wireless Communications and Mobile Computing*, *2021*(1), 6672297.

182. Ryu, J., Lee, H., Lee, Y., & Won, D. (2022). SMASG: Secure mobile authentication scheme for global mobility network. *IEEE Access*, *10*, 26907-26919.

183. Zagrouba, R., & Kardi, A. (2021). Comparative study of energy efficient routing techniques in wireless sensor networks. *Information*, *12*(1), 42.

184. Liu, M., Tian, M., Chen, X., & Wu, J. (2020). A Reliable Transport Scheme for Human Opportunistic Networks. *Applied Sciences*, *10*(19), 6658.

185. Ji, M., Cui, X., Li, J., Xu, T., Li, S., & Liu, J. (2021). A routing algorithm based on network connectivity assessment for maritime opportunistic networks. *Procedia Computer Science*, *187*, 200-205.

186. Chancay-García, L., Hernández-Orallo, E., Manzoni, P., Vegni, A. M., Loscri, V., Cano, J. C., & Calafate, C. T. (2020). Optimising message broadcasting in opportunistic networks. *Computer Communications*, *157*, 162-178.

187. Fernando, X., & Lăzăroiu, G. (2023). Spectrum sensing, clustering algorithms, and energy-harvesting technology for cognitive-radio-based internet-of-things networks. *Sensors*, *23*(18), 7792.

188. Hasan, S., Sharifi Sani, M., Iranmanesh, S., Al-Bayatti, A. H., Khan, S., & Raad, R. (2023). Enhanced message replication technique for DTN routing protocols. *Sensors*, *23*(2), 922.

189. Bozorgzadeh, E., Barati, H., & Barati, A. (2020). 3DEOR: an opportunity routing protocol using evidence theory appropriate for 3D urban environments in VANETs. *IET Communications*, *14*(22), 4022-4028.

190. Jardak, N., & Jault, Q. (2022). The potential of LEO satellite-based opportunistic navigation for high dynamic applications. *Sensors*, *22*(7), 2541.

191. Madni, M. A. A., Iranmanesh, S., & Raad, R. (2020). DTN and Non-DTN routing protocols for inter-cubesat communications: A comprehensive survey. *Electronics*, *9*(3), 482.

192. Khalil, A., & Zeddini, B. (2024). Cross-Layer Optimization for Enhanced IoT Connectivity: A Novel Routing Protocol for Opportunistic Networks. *Future Internet*, *16*(6), 183.

193. Yamini, K. A. P., Stephy, J., Suthendran, K., & Ravi, V. (2022). Improving routing disruption attack detection in MANETs using efficient trust establishment. *Transactions on Emerging Telecommunications Technologies*, *33*(5), e4446.

194. Sharma, V., You, I., Andersson, K., Palmieri, F., Rehmani, M. H., & Lim, J. (2020). Security, privacy and trust for smart mobile-Internet of Things (M-IoT): A survey. *IEEE access*, *8*, 167123-167163.

195. Mucchi, L., Jayousi, S., Caputo, S., Panayirci, E., Shahabuddin, S., Bechtold, J., ... & Haas, H. (2021). Physical-layer security in 6G networks. *IEEE Open Journal of the Communications Society*, *2*, 1901-1914.

196. Mahajan, S., Harikrishnan, R., & Kotecha, K. (2022). Adaptive routing in wireless mesh networks using hybrid reinforcement learning algorithm. *IEEE Access*, *10*, 107961-107979.

197. Taleb, S. M., Meraihi, Y., Gabis, A. B., Mirjalili, S., Zaguia, A., & Ramdane-Cherif, A. (2022). Solving the mesh router nodes placement in wireless mesh networks using coyote optimization algorithm. *Ieee Access*, *10*, 52744-52759.

198. Seo, Y. D., & Cho, Y. S. (2021). Point of interest recommendations based on the anchoring effect in location-based social network services. *Expert Systems with Applications*, *164*, 114018..

199. Xia, J., Fan, L., Yang, N., Deng, Y., Duong, T. Q., Karagiannidis, G. K., & Nallanathan, A. (2020). Opportunistic access point selection for mobile edge computing networks. *IEEE Transactions on Wireless Communications*, *20*(1), 695-709.

200. Pirmagomedov, R., Moltchanov, D., Samuylov, A., Orsino, A., Torsner, J., Andreev, S., & Koucheryavy, Y. (2022). Characterizing throughput and convergence time in dynamic multi-connectivity 5G deployments. *Computer Communications*, *187*, 45-58.

201. Trifunovic, S., Kouyoumdjieva, S. T., Distl, B., Pajevic, L., Karlsson, G., & Plattner, B. (2017). A decade of research in opportunistic networks: challenges, relevance, and future directions. *IEEE Communications Magazine*, *55*(1), 168-173.

202. Dalal, R., Khari, M., Anzola, J. P., & García-Díaz, V. (2021). Proliferation of opportunistic routing: A systematic review. *IEEE access*, *10*, 5855-5883.

203. Cao, Y., & Sun, Z. (2012). Routing in delay/disruption tolerant networks: A taxonomy, survey and challenges. *IEEE Communications surveys & tutorials*, *15*(2), 654-677.

204. Vahdat, A., & Becker, D. (2000, April). *Epidemic routing for partially connected ad hoc networks*.

205. Lindgren, A., Doria, A., & Schelen, O. (2004, August). Probabilistic routing in intermittently connected networks. In *International Workshop on Service Assurance with Partial and Intermittent Resources* (pp. 239-254). Berlin, Heidelberg: Springer Berlin Heidelberg.

206. Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2005, August). Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking* (pp. 252-259).

207. Dede, J., Förster, A., Hernández-Orallo, E., Herrera-Tapia, J., Kuladinithi, K., Kuppusamy, V., ... & Vatandas, Z. (2017). Simulating opportunistic networks: Survey and future directions. *IEEE Communications Surveys & Tutorials*, *20*(2), 1547-1573.

208. Keränen, A., Ott, J., & Kärkkäinen, T. (2009, March). The ONE simulator for DTN protocol evaluation. In *Proceedings of the 2nd international conference on simulation tools and techniques* (pp. 1-10).

209. Avoussoukpo, C. B., Ogunseyi, T. B., & Tchenagnon, M. (2021). Securing and facilitating communication within opportunistic networks: a holistic survey. *IEEE access*, *9*, 55009-55035.

210. Lilien, L., Kamal, Z. H., Bhuse, V., & Gupta, A. (2007). The concept of opportunistic networks and their research challenges in privacy and security. *Mobile and wireless network security and privacy*, 85-117.

211. Wu, Y., Zhao, Y., Riguidel, M., Wang, G., & Yi, P. (2015). Security and trust management in opportunistic networks: a survey. *Security and Communication Networks*, *8*(9), 1812-1827.

212. Farrell, S., & Cahill, V. (2006, July). Security considerations in space and delay tolerant networks. In *2nd IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06)* (pp. 8-pp). IEEE.

213. Wu, B., Chen, J., Wu, J., & Cardei, M. (2007). A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless network security* (pp. 103-135). Boston, MA: Springer US.

214. Asokan, N., Kostiainen, K., Ginzboorg, P., Ott, J., & Luo, C. (2007, June). Applicability of identity-based cryptography for disruption-tolerant networking. In *Proceedings of the 1st international MobiSys workshop on Mobile opportunistic networking* (pp. 52-56).

215. Xia, F., Liu, L., Li, J., Ma, J., & Vasilakos, A. V. (2013). Socially aware networking: A survey. *IEEE Systems Journal*, *9*(3), 904-921.

216. Hu, X., Chu, T. H., Leung, V. C., Ngai, E. C. H., Kruchten, P., & Chan, H. C. (2014). A survey on mobile social networks: Applications, platforms, system architectures, and future research directions. *IEEE Communications Surveys & Tutorials*, *17*(3), 1557-1581.

217. Guan, P., & Wu, J. (2019). Effective data communication based on social community in social opportunistic networks. *IEEE Access*, *7*, 12405-12414.

218. Karamshuk, D., Boldrini, C., Conti, M., & Passarella, A. (2011). Human mobility models for opportunistic networks. *IEEE Communications Magazine*, *49*(12), 157-165.

219. Musolesi, M., & Mascolo, C. (2007). Designing mobility models based on social network theory. *ACM SIGMOBILE Mobile Computing and Communications Review*, *11*(3), 59-70.