DESTRUCTION OF ATTACKS WITH MH^2-AODV ROUTING PROTOCOL IN VEHICULAR AD-HOC NETWORK

Synopsis –

Vehicular Ad-hoc Networks (VANET) are inaugurating for the purpose of communication among the moving vehicles over a constrained environment. Vehicles are subjected to move at high speed and hence they often face changes in their topology and frequent disconnections [1]. Due to these reasons routing remains as the major challenge in VANET. And one more challenge is that providing security, since various attacker's involvement in the network will degrade the network performance. Hence enormous routing and security related algorithms / methods were proposed in state–of–the–art research work. VANET also involves with grouping of vehicles, which is said to be as clustering.

In [2] clustering is focused, a vehicle with low average relative mobility and more number of followers was selected as cluster head. Here the isolated vehicles forms separate clusters, which increases the number of cluster head and increases the communication cost. Then in [3] Vehicular Multihop algorithm for Stable Clustering (VMaSC) was designed in which the header is selected with the least mobility, here the mobility calculation requires the support of GPS which consumes power and also increases the network traffic. Clustering may also ignore some nodes ideal. Then in [7] a reliable trust-based platoon service recommendation scheme (REPLACE) was proposed to avoid the selection of malicious platoon head vehicles. This scheme involves with a reputation system which collects and models the vehicle's feedbacks. Here the quality of the feedbacks are also estimated and filters out the untruth feedbacks. As per the speed of each vehicle it becomes difficult to select a trusted platoon head vehicle.

Routing in VANET was based on Modified AODV (MAODV) [4], in which the shortest path is selected for packet transmission, but if there occurred any fault then the routing path reconstruction is performed by source node; it means that the same process should be repeated. This MAODV based routing consumes more amount of time. Then MAODV protocol was designed to detect black hole attack [5]. Here two RREPs are generated for the purpose of identifying the attacker node. This cannot be maintained secure all the time since, the attacker node also has the possibility to generate RREP twice. In VANET to maintain security, an enhanced security scheme was built in [8]. The scheme introduced was, Identity – based Batch Verification (IBV) Scheme. In this scheme vehicle's identity is only taken in account, but even the malicious node has identity. To overcome all these constraints we move upon to our new proposal of routing protocol by which we overcome from two different attacks.

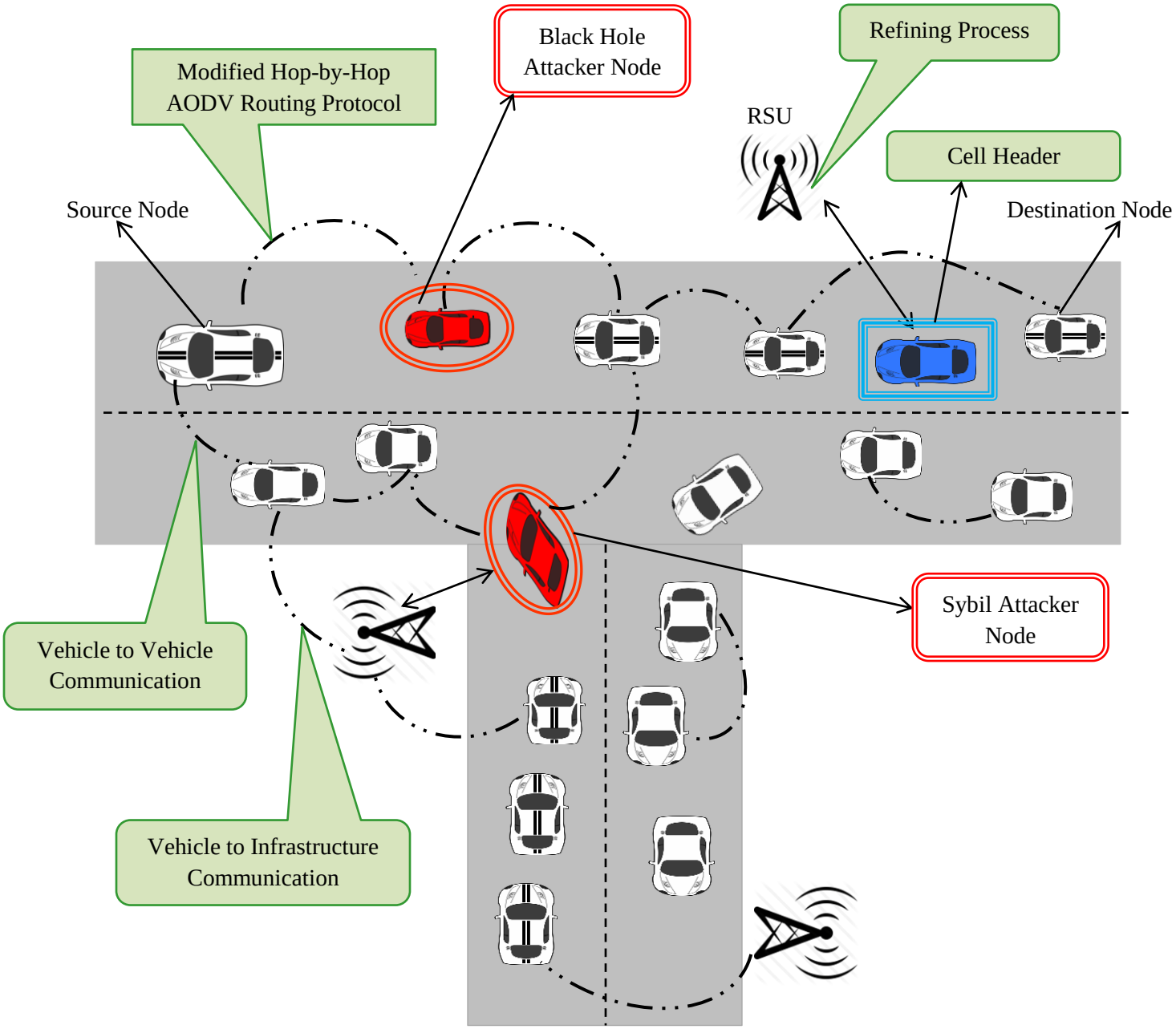
Our proposal starts with the grid formation to overcome the drawbacks faced during the cluster formation [2], [3]. Based on the area of the road segments the grid is formed with *'n'* number of cells and *'n'* number of Cell headers. The node with minimum mobility is selected as cell header by Road Side Unit (RSU). Next we perform routing by a novel routing protocol named ***Modified Hop-by-Hop AODV Routing Protocol (MH^2-AODV)***. This routing protocol involves with two steps one is Local testing and other is Refining process. Route request (RREQ) is flooded from the source node along with Source IP address, Source ID, Destination IP address, Source Sequence Number, Destination Sequence Number and Hop Count. Two paths are selected by the source node in which one path is stored temporarily.

Local testing is the first step in routing, performed for the purpose of selecting secure path from the source to destination. In this step the neighboring nodes reply for the route request with (RREP) packets. Each neighboring node first verifies the sequence number of the node, if that is greater than the destination sequence number then the node's RREP packet is detected whether a malicious packet or normal packet [6]. Generally the black hole attacker nodes have larger sequence number. Hence the malicious packet is detected by means of the vehicle's frequency and velocity. If the RREP are genuine then they are selected as intermediate nodes. We select two routes one is ***transmission route*** and another one is ***proxy route***. This Proxy route is utilized in case if the transmission route is broken, due to this the time for re-routing is reduced. Hereby in this step we overcome the ***Black hole attack***.

After route selection, the second step is Refining process, which is performed by RSU for preventing from Sybil attack. Sybil attacker node generates fake information with multiple identities. The selected route is forwarded to RSU along with the identities of the intermediate nodes via the cell header. Next RSU sends ***Message Authentication Code (MAC)*** to all the intermediate nodes, if they are legitimate nodes they reply with ***Hash Message Authentication Code (HMAC)*** within the timestamp. If no reply is received then that particular node is detected as ***Sybil Attacker***. After this, RSU intimates the presence of an attacker node in the selected path. Then RSU broadcasts an alert to all the legitimate nodes present in the network through the cell header. If the route is completely secure without any attacker nodes, then the source node is intimated to start packet transmission. Then the packets are encrypted by the source node and transmitted towards the destination node in the selected path.

Finally this research work is completely a novel approach to secure the entire Vehicular Ad-Hoc Network from attacks. And which effectively overcome from two different attacks with the routing algorithm itself. In simple it can be said as two in one approach. This proposed work shows better improvements from the state – of – the – art's performance metrics of Packet Delivery Ratio, End-to-End Delay and Normalized Overhead.

OVERALL PROPOSED ARCHITECTURE



REFERENCES

[1] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) – An Overview and Challenges", ResearchGate, Journal of Wireless Networking and Communications, pp 29 – 38, 2013.

[2] Yuzhong Chen, Mingyue Fang, Song Shi, Wenzhong Guo, Xianghan Zheng, "Distributed multi-hop clustering algorithm for VANETs based on neighborhood follow", EURASIP Journal on Wireless Communications and Networking, pp 1 – 12, 2015.

[3] Seyhan Ucar, Sinem Coleri Ergen, Oznur Ozkasap, "Multihop-Cluster-Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination", IEEE Transactions on Vehicular Technology, pp 2621 – 2636, 2016.

[4] Siddlingappagounda Biradar, Prahlad Kulkarni, "Enhancing the Quality of Service using M-AODV Protocol in MANETs", IEEE, International Conference on Applied and Theoretical Computing and Communication Technology, 2015.

[5] Houda Moudni, Mohamed Er-rouidi, Hicham Mouncif, Benachir El Hadadi, "Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack", IEEE, 2016 International Conference on Information Technology for Organizations Development, pp 1 – 7, 2016.

[6] Abdul Quyoom, Raja Ali, Devki Nandan Gouttam, Harish Sharma, "A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)", IEEE, International Conference on Computing, Communication and Automation, pp 414 – 419, 2015.

[7] Hao hu, Rongxing Lu, Zonghua Zhang, Jun Shao, "REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET", IEEE Transactions on Vehicular Technology, pp 1 – 11, 2016.

[8] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", IEEE Transactions on Vehicular Technology, pp 1 – 12, 2015.

REFERENCES EXPLANATION

REFERENCE 1

Title – Vehicular Ad-Hoc Networks (VANETs) – An Overview and Challenges

Concept Explanation

This paper elaborates VANET architecture which is comprised of moving vehicles and Road Side Units. The vehicles participating in this network consists of an On-Board Units, wireless transmitter and receiver. Further it illustrates the major categories of routing which includes Topology Driven Protocols, Location based Routing protocols, Cluster based Protocols, Broad cast Protocols and Geo cast Protocols. Each category of routing protocol involves with sub – classification of routing. The major research areas in VANET are Quality of Service, Scalability, Robustness, Authentication and Security, Cooperative communication and also designing efficient routing algorithms. Based on all these challenges each research work is constructed. This paper completely gives up an introduction of VANET.

REFERENCE 2

Title – Distributed multi-hop clustering algorithm for VANETs based on neighborhood follow

Concept Explanation

This paper involves with clustering of the vehicles present in VANET. A cluster model was designed based on one-hop neighborhood follow strategy. This strategy was designed to select the vehicles and thereby to follow the target vehicles from one – hop neighbors. By using this strategy clusters are formed and maintained in distributed manner. A cluster head is selected which consists of more number of followers and smaller average relative mobility. Here in case if one or two vehicles which stay isolated will form a separate cluster. This causes some drawbacks which leads to the degradation of the network performance.

Drawback

- Increase in number of Cluster head and communication cost
- Decreases routing Efficiency
- Nodes have the possibility to be left ideal

Proposed Work

- Grid formation (Covers all the vehicular nodes)
- One cell header for one cell

REFERENCE 3

Title – Multihop–Cluster–Based IEEE 802.11p and LTE Hybrid Architecture for VANET Safety Message Dissemination

Concept Explanation

This paper proposed Vehicular Multihop algorithm for stable Clustering (VMaSC) approach. Based on the relative mobility of the vehicle a cluster head is selected. The relative mobility is computed with the support of GPS, by identifying the speed of the vehicle and its neighboring vehicle. Here cluster is constructed based on the major constraint of reducing overhead. Each vehicle maintains a Vehicle Information Base (VIB) for storing the vehicle's information. If this VIB is not updated then they are deleted. Here if the member vehicle in a cluster is decreased then it can be merged to another cluster by just sending a join request. The nodes present in the merging cluster should move in the same direction.

Drawback

- Use of GPS consumes more energy
- Reduces the nodes lifetime earlier
- Increases Network Traffic

Proposed Work

- Use Beacon messages for estimating the relative speed

REFERENCE 4

Title – Enhancing the Quality of Service using M-AODV Protocol in MANETs

Concept Explanation

This paper proposes an enhanced routing protocol that is Modified Ad-hoc On-Demand Distance Vector (M-AODV) routing. M-AODV involves with route discovery, route reply and then path is selected based on the minimum number of hop counts from the source node to the destination. In traditional AODV when a selected path is broken then there the path is repaired by the intermediate nodes, whereas

in this M-AODV the source node retries with the RREQ hello packets. On the comparison of AODV with M-AODV it shows only a slight variation in throughput, packet delivery ratio and energy consumption.

Drawback

- If a path is broken, it takes up time for reconstruction of path

Proposed Work

- Our proposed protocol selects two paths
- If a path is broken it starts transmission in the selected Proxy route
- No need for reconstruction of path

REFERENCE 5

Title – Modified AODV Routing Protocol to Improve Security and Performance against Black Hole Attack

Concept explanation

In this paper Modified – AODV is designed to fight against Black hole attack. The source node starts broadcasting RREQ packet to all its available neighboring nodes to find the destination. In traditional AODV protocol only one RREP is generated, but in this paper two RREP packets are generated for the purpose detecting the black hole attacker node. On receiving the RREQ packets the node's reply with first RREP packets then they increment 1 to the sequence number and send the second RREP packets. The increment of the sequence number in the RREP packets is verified and then if packets satisfy this constraint then it is forwarded to the next hop node. By this the on verifying the sequence number of RREP packets the black hole attacker node is detected.

Drawback

- Not applicable at all times
- Avoids only black hole attack
- Possibility to generate RREP twice by Attacker node

REFERENCE 6

Title – A Novel Mechanism of Detection of Denial of Service Attack (DoS) in VANET using Malicious and Irrelevant Packet Detection Algorithm (MIPDA)

Concept Explanation

This paper describes the possible attacks in VANET; they are Broadcast Tempering, Denial of Service attack, Sybil attack, Jamming attack, Message Suppression attack and sending false information. It is clear that the Sybil attack occurs by which the attacker node perform forgery with the identity. In this paper the packet are classified into three categories such as Malicious packet / Invalid Packet, Irrelevant Packet and Real packets. The Malicious packets are identified by the frequency and velocity. If the ranges of the frequency and velocity are either too low or too high, then those packets are detected as malicious packets or invalid packets.

REFERENCE 7

Title – REPLACE: A Reliable Trust-based Platoon Service Recommendation Scheme in VANET

Concept Explanation

This paper proposes REPLACE scheme for the selection of trusted vehicle as the platoon head in the Vehicular Ad-hoc Network. This scheme involves with five major steps to be followed they are System initialization, Quality of feedbacks computation, Dirichlet-based model, trustworthiness of user vehicles and reputation of the Platoon Head vehicles. In first system initialization the keys are generated for the corresponding vehicles, and then the server will establish a feedback table which is collected from all the vehicles. Further we compute the quality of the feedbacks by filtering out the untruth feedbacks. The Dirichlet-based model is for measuring the uncertainty of feedbacks based on the historical data. Weights are assigned for each satisfactory level and based on the weights and cumulative evidences the user vehicle's trustworthiness is estimated. Finally the reputation of the Platoon Head vehicle is computed by aggregating the entire trusted user vehicle's feedback.

Drawback

- Takes up more time
- It is difficult to maintain same trusted PH for larger time period
- Due to the change of PH, often computation should be performed

Proposed Work

- Minimum time for the selection of cell header

REFERENCE 8

Title – Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET

Concept Explanation

This paper proposed an Identity based Batch Verification (IBV) scheme for the purpose of securing the vehicular nodes from attacks. This scheme consists of three major phases they are system initialization, anonymous identity generation, and message signing and message authentication. In the first system initialization phase the trusted authority computes private key and public key. Then it chooses two hash functions and assigns a real identity and password for each vehicle. In second phase the unique real identity is verified. After completion of this verification it generates an anonymous identity which contains two parts. Next, third phase involves with single verification of one message and Batch verification of multiple messages.