Literature Survey on the Destruction of Attacks with Mh Hop to Hop-Aodv Routing Protocol in Vehicular Ad-Hoc Network

K Phani Srinivas[1], Dr.K.Sai Manoj[2], Mrudula Kudaravalli[3]
[1]*Head R&D, Amrita Sai Institute of Science and Technology, Paritala, AP, India*
[2]*CEO, Amrita Sai Institute of Science and Technology, Paritala, AP, India*
[3]*Assistant Professor, Amrita Sai Institute of Science and Technology, Paritala, AP, India*

Abstract- **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**

I. INTRODUCTION

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.

II. LITERATURE SURVEY REGARDING THIS WORK

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.

III. CONCEPT RELATED TO THE WORK

This 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 (MH2-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.

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] [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.