Malicious Node Detection in VANET Using Admission Control Algorithm (ACA)

J. Sivapriya[1], PG Scholar, sivapriyajayakumar90@gmail.com

N. Jothy[2], Assistant Professor, njothy2005@gmail.com

Sri Manakula Vinayagar Engineering College, Puducherry, India

Abstract: **Vehicular ad hoc networks (VANET) is a class of ad hoc networks that consist of vehicles and Roadside Units (RSU). VANET were originally created to enhance safety on the road using cooperative collision warning via Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. Network management, congestion and collision control, environmental impact, MAC design and security are the challenging issues in VANET. Ensuring secure and trusted communications within vehicular ad hoc networks (VANET) is a complex task due to the different threats to be addressed. For this purpose, several trust models have been proposed to ensure security of VANET by identifying dishonest vehicles and revoking messages with malicious content. In the existing work event oriented Hybrid Trust Model (HTM) known as Vehicular Security through Reputation and Plausibility Check (VSRP) algorithm to quickly identify and isolate adversaries from the network. The limitation on this work is, it only identifies malicious node in black hole attack in V2I communication. In the proposed work, instead of maintaining long records of node details in central trusted authority, using admission controller, generate a random password by making trusted communication between V2V and also to detect malicious node in worm hole attack.**

Keywords — Vehicular Ad Hoc Network (VANET), Vehicle-To-Vehicle (V2V) Communication, Vehicle-To-Infrastructure (V2I) Communication, Vehicular Security Through Reputation And Plausibility Check (VSRP).

I. INTRODUCTION

VANET is a mobile based ad hoc network employed in a dsrc band in a frequency of 5.9 ghz.in VANET exchange of text messages among the vehicles is occurring in a secured manner using trust platform module (tpm) .in VANET exchange of information between the vehicles is repeated one. There is the possibility of having malicious vehicle in the network. The malicious one will take step in advance to hack the key/messages from legal node. So the legal one has to check the communicating node frequently. Each nodes participating in the network is given a specific identity number to be discovered by the neighbors. An extended list is managed by the (cta) central trusted authority to monitor the vehicle nodes. This list may grow larger in proportions and it will take too much of time to check the identity of a specific communicating node. The central trusted authority will distribute a random password to the vehicle mobile nodes. When one node is certainly attempting to have interaction with the legal node, the legal one will handle the random password test. The communicating node also should pass the random password test. If the node passes the check then it'll be declared as a legal one and conversation demand will be accepted and message sharing will take place. If the communicating node fails to pass the random password test, it is declared as a malicious one and communication with that node is banned completely so that staying of malicious nodes in the network will be saved from it. The random password may be of any desired length. Basically attacks can be classified in to black hole and worm hole attack. Once THE VEHICLE enters in the network it will be checked by cta and if the node is identified as malicious then the attack is said to be black hole. All the nodes present in network after checking in secure range can be transformed in to malicious due to any situation then it is said to be worm hole.

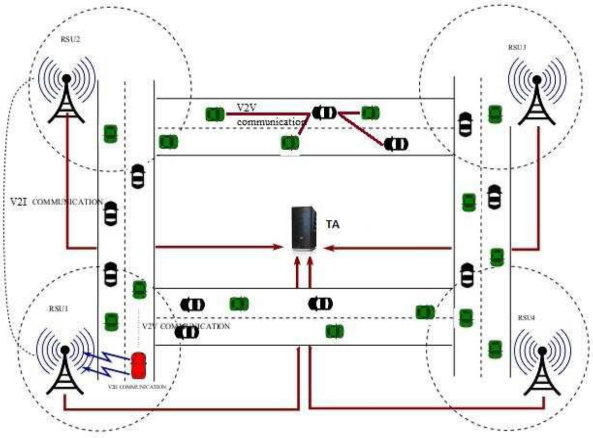

Fig 1.The structure of VANET

II. RELATED WORK

In [1] Farhan Ahmad et al. proposed a novel Trust Evaluation and Management (TEAM) framework, which serves as a unique paradigm for the design, management and evaluation of TMs in various contexts and in presence of malicious vehicles. Our framework incorporates an asset-based threat model and ISO-based risk assessment for the identification of attacks against critical risks. TEAM has been built using VEINS, an open source simulation environment which incorporates SUMO traffic simulator and OMNET++ discrete event simulator. The framework created has been tested with the implementation of three types of TM (data oriented, entity-oriented and hybrid) under four different contexts of VANET based on the mobility of both honest and malicious vehicles. Results indicate that TEAM is effective to simulate a wide range of TMs, where the efficiency is evaluated against different Quality of Service (QoS) and security-related criteria. Such framework may be instrumental for planning smart cities and for car manufacturers. In [2] D. jiang, et al, proposed that VANET works on the DSRC band of 5.9 GHz bandwidth in order to have faster communication among the nodes, because the slower communication will lead to fatal accidents. If the message is not sent at a correct time the information will reach the vehicle only at later part of time after the accident is met .So DSRC is a best mode for communicating in a proper manner. The DSRC is divided into seven 10 MHz wide channels. Channel 178 is the control channel restricted for safety communication mode. The channels at the edges of the spectrum are meant for the advanced accident avoidance. The remaining channels are used for safety and non-safety usage.

In [3], A.A.Wagan, et al, proposed that TPM is a hardware enabling secured communication among the nodes using both symmetric TESLA and asymmetric ECDSA algorithms. TESLA is used for the key generation quickly and the ECDSA is used for the secured communication between the nodes. The TPM uses two keys public and private keys. The private key is known only to the user and public key is supplied to all others. At the sending end the digital signature is created and encrypted and at the receiving end the reverse process takes place and decrypted. In [4], P.Golle, et al, proposed that malicious node try to hack the secret keys/messages of legal nodes present in a list maintained by CTA and distribute to all the malicious Vehicle node. In [5], B.xiao, et al, proposed that there are possibilities of having Sybil nodes that will take step ahead to spear the secret keys /messages from the legal nodes. A Sybil attack is nothing but trying to hack the messages without the permission of the legal node in an illegal way.

In [6], M.Bohge et al, said that TESLA is a broadcast authentication technique having asymmetric properties in spite of using purely symmetric cryptographic feature. TESLA is based up on delayed key disclosure. TESLA has low computation cost. The technique is used to takeoff the false certification before key disclosure. In [7], Ram Shringar Raw et al. discussed about the VANET and its technical and security challenges. And also they discussed some major attacks and solutions that can be implemented against these attacks. They compared the solution using different parameters. Lastly they discussed the mechanisms that are used in the solutions.

In [8], Jorge H. et al, proposed watchdog algorithm with intrusion detection techniques for establishing trust management. In that source node sent packets to the neighbor node are monitored the other node with ids. Its forward that packets than maintain its trust value in trust table otherwise that decrease trust value of that node. Drawback of this technique is to create collision in network, and monitor that node until that forward or drop. It has contained huge monitoring history of neighbor node if it has large number of neighbor nodes. In [9], Cong et al, proposed trustworthiness based on incident reports in V2V communication and forward to those vehicles. Crowd sourcing capabilities use for evaluating trustworthiness value for vehicles. Global view can broadcast for individual vehicles trust value in CSC. Future work includes security and privacy issues using unique identification and public key infrastructure mechanism. In [10], J.Serna, et al, created MACM (Mandatory Access Control Model) and a novel architecture for trust propagation. The MACM specific who has what type of access to which targets and under which conditions. The novel architecture for trust propagation to get information about the certify authorities and attribute authorities valid for specific geographical area.

In [11] Subir. B et al, proposed id-based techniques used for verification of cars with public key without certificate. Proxy server provide message authentication and trust management. Safety message delivered though RSU (rode site unit) and id-based signature properties implies on proxy signature with ECDSA. In this technique authentication and trust management is dynamic and un-trustworthiness. Trust management scheme is handled by RSU which had proxy signature pre-stored.

III. EXISTING SYSTEM

In this system Vehicular security through reputation and plausibility checks (VSRP) is discussed. This algorithm is used to prevent attacks based on false event generation, event modification, data aggregation and data dropping. The first two attacks are identified by its own sensors. Later data aggregation and dropping are the attacks processed by VSRP algorithm. Data aggregation attack means neighbor vehicle floods the neighbor request packets to confuse the legitimate user Neighbor request packet is received from same node, counter maintained is incremented by one, if it exceeds the threshold range then it is said to be malicious

DOI : 10.35291/2454-9150.2019.0036

by generating malicious intent packets. Data dropping attack naturally drops the information to be forwarded (blindly assumed to be malicious). These two drawbacks are overcome in the proposed algorithm. In this system to detect malicious node identity key present in the CTA, sender node has to check each and every position of the list. It will take vast time. Also it can able to detect only black hole attack type.

IV. PROPOSED WORK

Instead of using the long list of nodes with unique identities in the CTA we are going to use a Random password to the Vehicle nodes present in the list of CTA .For that purpose we are going to generate a Random password of desired length. A random Admission Controller (RAC) is either a software or a hardware device. It will take the input from a random or pseudo number generator and can generate the Random password vehicle automatically as an inbuilt function. An Admission Controller is one of the part of a Random password manager. The Random password-policy enforces complex rules. In this situation, it can be easier to use an Admission Controller based on that set of rules than to manually create Random passwords.

A random number generator (RNG) is device designed to generate a sequence of numbers or symbols that has any pattern i.e. they will appear random. An encryption engine placed inside the RAC generates a Random password of desirable bit length from the input taken from the RNG. This is an inbuilt feature .It assumes the key value for each letter/number from ASCII. Now the generated Random password is supplied to the under lying nodes. The figure 1 shows the architectural view of Random password generation and distribution.

1. Input is taken from the random number generator.
2. The encryption engine is placed inside the random Admission Controller and it converts the received input from the random or pseudo number generator to a Random password as an inbuilt function by assuming ASCII key values.

3.The generated Random password is then to the underlying nodes.

The block diagram will explain the distribution of Random password and how the trusted communication takes place among the nodes unknown to each other even they are Vehicle of a common CTA.

4.1 Random password generation:

Assume that a CTA node is generating Random password of n length.

Allowable characters are, Letters=A....Z,

Numbers=O....9, Special characters,

On giving the Random password, corresponding ASCII code will be given as output.

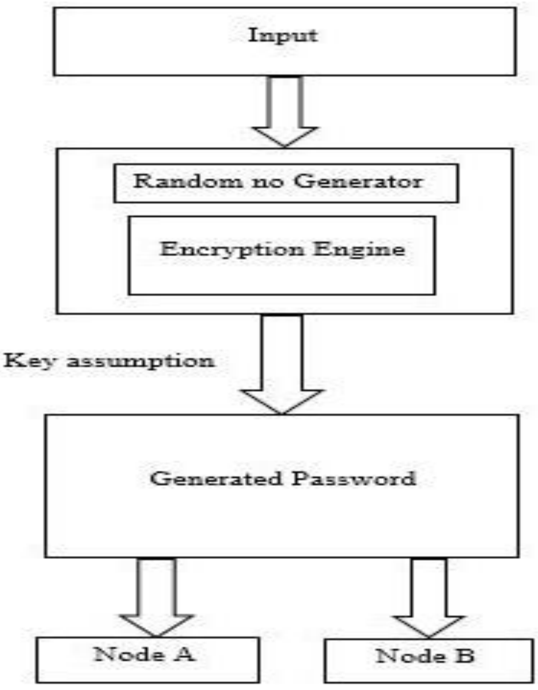

Fig.2 Architectural view of password generation and distribution.

4.2 Random password verification:

Compare the Random password given by communicating node with Random password given by CTA. If matched, then communication request is accepted. If mismatched, then reject the communication request. Send vigil information about that node to neighbors.

4.3 ACA ALGORITHM

STEP 1: Initialization

STEP 2: Node formation

STEP 3: Sending dummy packets to all nodes

STEP 4: Getting ACK from all the nodes

STEP 5: From ACK, calculate packet loss rate of each node by using trust value

STEP 6: If trust value is below 70% then it is identified as malicious node

STEP 7: Getting the input from Pseudo Random Number Generator

STEP 8: Using node position random number is generated
STEP 9: Distribution of password to all nodes by Central Trusted Authority with time stamp.

V. SIMULATION RESULTS AND DISCUSSION

In this segment by means of ns2 simulator, comparison between VSRP algorithm and ACA algorithm is shown below. In this simulation, percentage of malicious node

DOI : 10.35291/2454-9150.2019.0036

detection and performance metrics is compared in case of both VSRP and Admission control algorithm. Performance metrics analyzed are, Packet delivery ratio (PDR), Throughput, Trust factor, and malicious node identification. The simulation parameter are presented in the Table 1.

PARAMETER	VALUE
Routing Protocol	AODV
Channel Type	Wireless Channel
No. of nodes	30
Transport Protocol	TCP
Packet Size	512 Kb
Area of simulation	1500m X 1500m
Maximum Bandwidth	1 Mbps
Simulation Time	20ms
Traffic type	CBR
Threshold	70 to 100%

Table 1. Simulation parameters

5.1 PACKET DELIVERY RATIO

It is the ratios of the number of packets that are successfully delivered to destination compared to the number of packets have been sent by the sender.

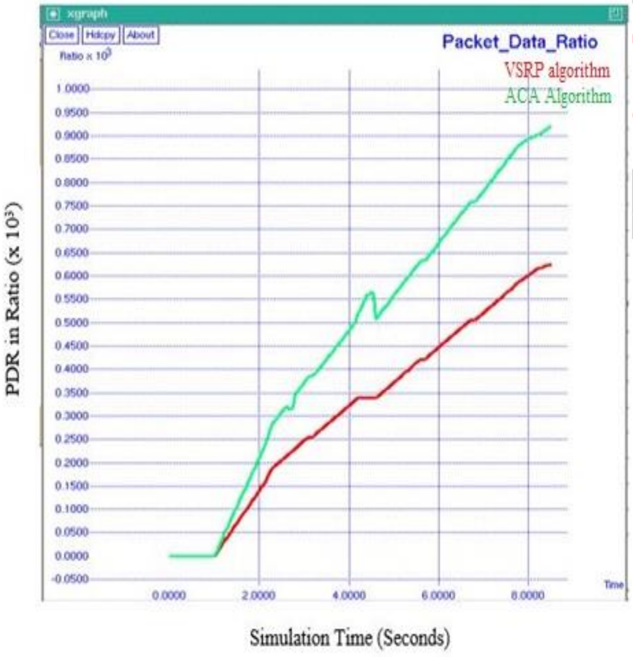

Fig 3. Packet Delivery Ratio

In the fig 3, the packet delivery ratio of VSRP algorithm and ACA algorithm with number of nodes under general conditions of simulation scenario. It is clear from the graph that when packet drop nodes are identified earlier in the PDR of ACA algorithm is better than of VSRP algorithm.

5.2 THROUGHPUT

Number of bits receives by destination node per unit time. It is measured in kilobits per second (kbps).

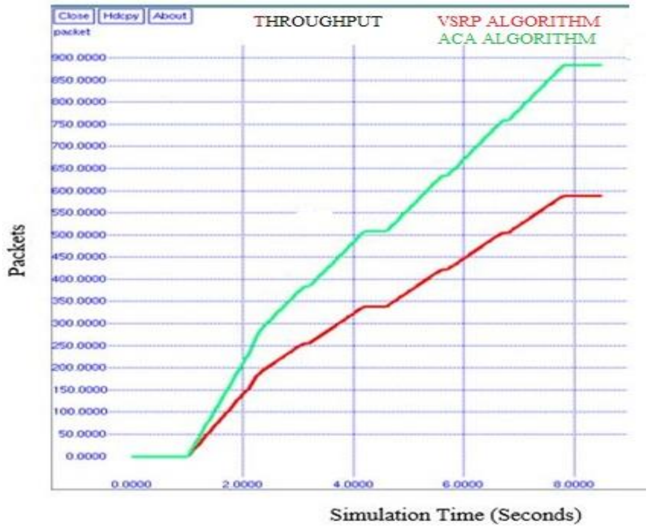

Fig 4. Throughput

The above fig 4 shows the throughput of VSRP algorithm and ACA algorithm with number of nodes under general conditions of simulation scenario. It is clear from the graph that attacker free environment provides the throughput of ACA algorithm is increases than that of VSRP algorithm. Number of received packet increases with time in ACA algorithm.

5.3 TRUST FACTOR

It is the calculation of trust for every node present in the network to isolate malicious node early.

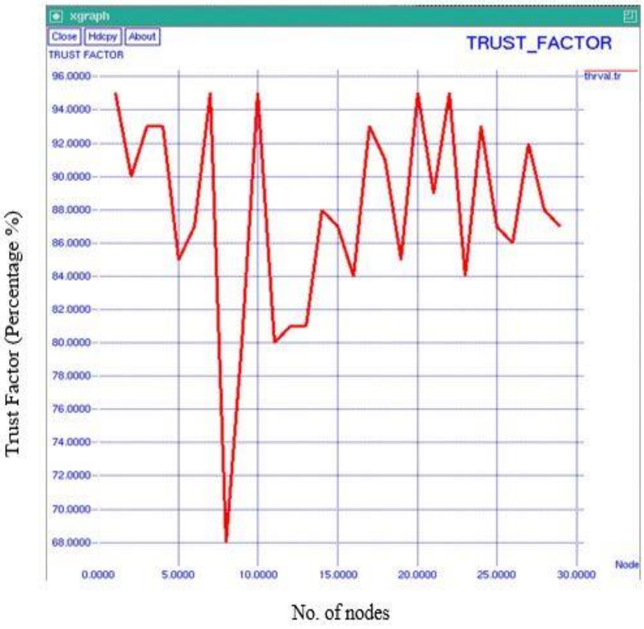

Fig 4.Trust Factor of Single Node

DOI : 10.35291/2454-9150.2019.0036

The above fig 4 shows the trust factor of Admission control algorithm (ACA) with number of nodes under general conditions of simulation scenario. It is clear from the graph that the trust of 8th node is below 70%, so that this node is declared to be malicious.

5.4 PERCENTAGE OF MALICIOUS NODE DETECTION

PDR ratio decreases when there is a malicious node in the network because some of the packets are dropped by the malicious node.so % of malicious node should be decreased by the proposed algorithm.

While sending dummy packets in the network to identify malicious node, the dropping of pkts is larger in VSRP algorithm, where in ACA algorithm is smaller, is identified using % of malicious node detection.

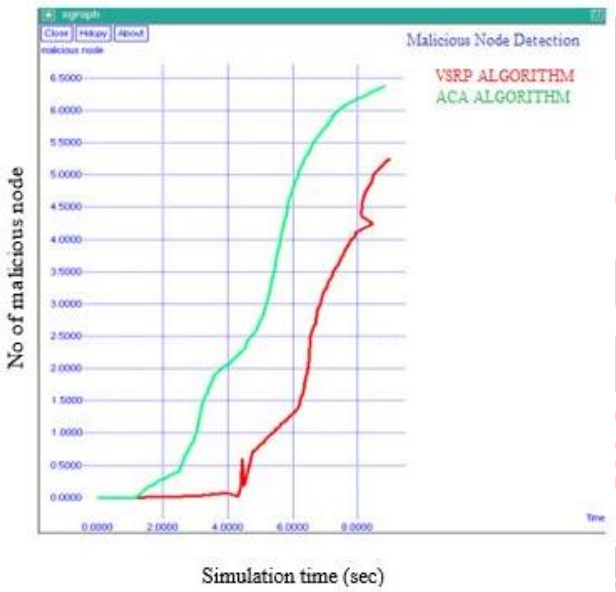

Fig 5. Percentage of Malicious Node Detection

The above fig 5 shows the percentage of malicious node detection of Admission control algorithm with number of nodes under general conditions of simulation scenario. It is clear from the graph that the detection of malicious node in ACA algorithm increases because of trust factor of each node analysis than VSRP algorithm with respect to time.

VI. CONCLUSION

The performance of VSRP and ACA algorithm is analyzed using ns-2.28. These algorithms were compared in terms of packet delivery ratio, Throughput, and percentage of malicious node identification. The Random password is created in the Central Trusted Authority and this Random password is shared with the nodes that are legally present in the list and trusted communication takes place among these nodes. So that both black hole and worm hole attacks are cleared in the network. The pseudonym generation is used for secured transmission. Admission Control achieves the desired authentication, privacy preservation, non-repudiation and other security objectives in VANETs. Another important characteristic of Admission Control is its reusability, i.e. it can also be utilized with other new schemes for security and performance improvements. Analysis and performance evaluation show that, the proposed Admission Control is feasible and adequate to UVC in the VANET environment. In future, the proposed model can be used in other routing attack to find out the performances. In future global trust table may be introduced to enhance the proposed model performances.

REFERENCES

[1] Farhan ahmad, virginia .N, L. Franqueira, and Asma adnane, "Team: A trust evaluation and management framework in context-enabled vehicular ad-hoc networks". IEEE access, vol. 4, pp. 2169 – 3536, 2018.

[2] D. jiang , V. Tliwaal , A Meier and Holfelder, "Design of 5.9 GHz DSRC-based vehicular safety communication", IEEE Wireless Communications, vol-3, no. 5, pp.36-43, October 2006.

[3] A. Wagan, B.M.Mughal, H.Hasbullah, "VANET security for trusted grouping using TPM hardware", Se International conference on communication software and networking 2010.

[4] P. Golle, D. Greene, Staddon, "Detecting and Correcting Malicious Data in VANETs" Philadelphia, Pennsylvania, USA, October 1, 2004.

[5] B.Xiao, B. Yu, C. Gao," Detection and Localization of Sybil Nodes in VAN Los Angeles, California USA, DIWANS'06, September 26, 2006.

[6] M. Bohge, W. Trappe, "TESLA Certificates: An Authentication Tool for Networks of compute-Constrained Devices ", In ACM workshop on wireless security (WISE'03) San Diego, CA, USA, August 2003

[7] Ram Shringar raw, Manish Kumar and Nan hay Singh, "Security challenges, issues and their solutions for VANET", International journal of network security & its applications (IJNSA), vol.5, no.5, September 2017.

[8] Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs", In Communications Workshops (ICC), IEEE International Conference on, pp-1-5. 2015.

[9] Liao, Cong, Jian Chang, Insup Lee, and Krishna K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", In Wireless Vehicular Communications (WiVEC), IEEE 5th International Symposium on, pp-1-5, 2014.

[10] Serna, J. Luna, M.Medina,"Geolocation based trust for VANETs privacy", Journal of information assurance and security- June 10, 2009.

[11] Biswas, Subir, Jelena Misic, and Vojislav Misic, "ID-based safety message authentication for security and trust in vehicular networks", In Distributed Computing Systems Workshops (ICDCSW), 31st IEEE, International Conference on, pp.- 323-331, 2011.