IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. IV (May-Jun. 2016), PP 60-67
www.iosrjournals.org

Vehicular Adhoc Network (VANETs) Security Enhancement Using Autonomic Framework and Trust Based Routing Algorithm

Sunita Karande[1], Govindkumar Lohiya[2]
[1,2](Electronics and Telecommunication, Datta Meghe College of Engineering/ Mumbai University, India)

Abstract: *The security protocols in the area of Vehicular Ad-hoc Networks (VANETs) have gained an immense importance from the research community. A noteworthy improvement in the research associated to trust management in the VANETs is detected. The security, privacy and safety of private user information are the prime requirements for the deployment of the protocols in vehicular ad-hoc networks. Nodes in the VANETs network uses packet forwarding for smooth functionality of the network. Some selfish nodes avoid packet forwarding and save the network resources for their own interest or can broadcast malicious information in the network. To isolate these selfish nodes from taking part in the network communication Autonomic Trust and Reputation Monitoring Scheme (ATRMS) is proposed which provides security services like access control, authentication and malicious node detection. The proposed framework uses trust monitoring scheme based on autonomic principles with trust and reputation based data transfer protocol for trust management in VANETs. The proposed system gives associate uniform up-to-date trust information throughout the network with minimum overhead, and it also reduces the impact of double-face attacks.*
Keywords: *Trust, Reputation, VANETs, Autonomic, Security, Double-face attack, ATRMS*

I. Introduction

In country like India today's transportation system becomes inefficient because of increasing amount of vehicles. Year by year increase in the road accidents and traffic jams leads to loss of millions of lives. This is the major problem faced by the society today. Use of Vehicular Ad-hoc networks (VANETs) can be used to resolve the problem of vehicular safety as well as traffic control and optimization. VANETs consist of nodes equipped with on board units (OBUs) for wireless communication and road side units (RSUs). In VANETs both Vehicle to Vehicle and Vehicle to Infrastructure/ Vehicle to Road site unit communication can be possible.

Due to the VANETs self-organized nature and inadequate resources, nodes in a network can behave selfishly or maliciously for individual benefits, for example, nodes can refuse to forward packets. Trusting on a malicious node can lead to unpredicted hazards, like lowering network efficiency, large resource consumption and exposure to attacks. Hence, using trust management mechanism nodes can be allowed to assume how much they can trust on behavior of the other nodes.

Trust management has three main components: knowledge collection, trust level computation and trust establishment. [2] The node's behavior can be known using knowledge collection component. The computation component calculates trust level for each node based on the collected behavioral data or trust suggestion. The result is a trust level, which represents nodes trust about trustworthiness of other nodes. The trustworthiness establishment component concludes if a node can be trusted based on its trust level.

In the available trust management schemes trust can be evaluated based on local information and global information. For local information evaluation the individual experiences are collected by the nodes themselves on the behavior of the neighbors. Global information is collected by the recommendations, which consist opinion of other network nodes which provides trustworthiness of a given node. Existing trust management frameworks for VANETs are based on only local information obtained by promiscuous node and they are prone to double-face attackers, i.e. nodes that behave selfish in one position and normal in another position in order to remain hidden. The vulnerability of these attacks can be reduced by having the global information of the nodes.

As VANETs mainly deals with the road safety and traffic information, successful attack by malicious node can develop life threatening situation. Hence, security is a prime concern in VANETs as an attacker may try to modify or insert malicious information. The main attacks in VANETs are impersonation, in-transit traffic tampering, gray hole, worm hole, message forging, on-board tampering, and packet dropping.

VANETs are mainly used for the applications like passenger ease, comfort and safety but, the most important application of VANETs is to provide safe and secure road conditions to the passengers. For handling security in infrastructure based VANET mainly infrastructure is used, in real time private keys are provided to the vehicles. These keys require full support of infrastructure to work well. If these keys are stored on the vehicles attackers can misuse these keys.

However, security remains the main challenge in VANETs. In this paper, a framework which uses Autonomic Trust and Reputation Monitoring Scheme (ATRMS) based on autonomic principles and a trust and reputation based data transfer protocol for enhancing trust management and security in VANETs is proposed. Node's trustworthiness Knowledge is applied to data transfer protocol to find malicious nodes in the network. Nodes knowledge is evaluated using ATRMS, which can be obtained using local and global trust information.

This paper can be summarized as follows; Section II reports related works, discussing existing monitoring schemes and protocols. Section III presents proposed system, providing details about the proposed system. Section IV describes the security analysis of proposed algorithm. Section V presents the performance of proposed algorithm. Finally, section VI concludes the paper and mention future work.

II. Related Works

For enhancing VANET security an autonomic trust and reputation monitoring scheme which uses trust based data transfer protocol based on reputation and plausibility checks to establish trust relations between nodes in a VANETs. The proposed framework uses autonomic principles. Advantage of this framework is it's uniform distribution of trust values among the VANETs nodes.

Sanjay K. Dhurandher et. al [1] proposed a trust based algorithm which establishes security in a VANET through accomplishment of trust levels for nodes in the network using reputation and plausibility checks. The algorithm follows an event oriented approach, that is, a node initiates the communication when it observes an event through its sensors. The algorithm in the case of traffic jams and accidents was divided into four phases: neighbor discovery, data dispatching, decision making and trust updating, and neighbor monitoring. In the case of information related to brakes the algorithm was divided into three phases: data dispatching, decision making and trust updating, and neighbor monitoring. The protocol is efficient in detecting malicious nodes and handling various attacks.

Zeinab Movahedi et. al. [2] proposed a new knowledge monitoring scheme for MANETs trust management based on autonomic principles. Overhead minimization is done by using transiting packets on the network to update nodes knowledge about trustworthiness of other nodes. As per the results presented in the paper this scheme significantly improved performance of the network, providing a sufficient knowledge about trustworthiness of the nodes required by trust management frameworks.

Dotzer, F et al. VARS [3] proposed a reputation-based system which uses modules for direct and indirect reputation handling, opinion generation and confidence decision (message handling) and situation recognition. VARS defines three areas: the event area , the decision area and the distribution area which specifies area for message distribution. VARS used redundancy within the reputation system and high mobility in order to tackle the attacks. Simulations have proven it usable in face of fake events, up to some satisfying degree of malicious nodes. However sophisticated attacks, such as collusion attacks, cannot be handled because long-lasting group attackers can manipulate reputation database of the node.

Chen Chen et. al., [4] used a trust-based message propagation and evaluation framework. Where nodes share road safety information, others nodes provide opinions about whether the information is trustworthy or not. This trust-based message propagation model collects and propagates nodes opinions in an efficient, scalable and secure way by controlling information scattering. This trust-based message evaluation model allows nodes to evaluate the information in a distributed manner by taking into account opinion of others nodes. According to the results this framework provides system effectiveness in information evaluation under the false information presence.

Li et al. [5] stated that use of only local information provides an partial solution for trust management. Proposed an objective trust management framework based on direct as well as indirect information. Watchdog mechanism is used for obtaining the direct observation. The indirect information can be obtained periodically between nodes in the network and then used by other nodes. After the formation indirect information, it is provided in the network. After receiving this information a deviation test is conducted at the nodes and uses this trustworthiness as a weight whenever necessary. This mechanism confirms an uniform distribution of trust values in the network, and it generates large overhead to MANETs.

T.W. Chim et. al., [6] proposed a secure and privacy preserving navigation scheme. It gives advantage of real time route optimization as well as authentication of the information source. Anonymous credentials are used in this scheme to protect privacy of the destination. The security scheme used was pairing based and defined on a mapping called bilinear map. In the cryptographic schemes this pairing operation is the most expensive operation. Proxy re-encryption scheme is also used for securing the message from the RSUs. Secured data can be distributed by the RSUs while at the same time, it is kept secret from the RSUs. VSPN is efficient in completing whole navigation process and receiving the urgent notifications in short time period. On the other hand, compared with the offline approach the route returned by this scheme saves upto 55 percent of traveling time. This scheme also provides lower route blocking rate. Drawback of this scheme is that such a centralized approach is not scalable, especially for large cities. The scheme is effective in terms of processing delay and providing shorter traveling time.

III. Proposed System

The proposed system consists of Autonomic Trust and Reputation Monitoring Scheme (ATRMS), a knowledge monitoring scheme for trust management based on autonomic principles and a trust based data transfer protocol which uses reputation and plausibility checks to addresses security issue in VANETs. The proposed system provides security against the double face attack. The proposed system is divided into four modules: Trust Monitoring Scheme (TMS), Reputation and Plausibility Protocol Checks, Trust comparison & Malicious Node Identification Process and Isolation of Malicious Nodes and Neighbor Monitoring. The proposed system is shown in Fig. 1.

A Trust Monitoring Scheme based on autonomic principles is proposed for trust management. TMS is characterized by its protocol and trust framework independence, simplicity, self-adaptation, and low computational complexity. The system generates the Local and Global Trust tables for the nodes in the network. The main goal of the proposed system is to provide an uniform up-to-date trust knowledge within the network with a minimum observation overhead and reduce the impact of double-face attacks.

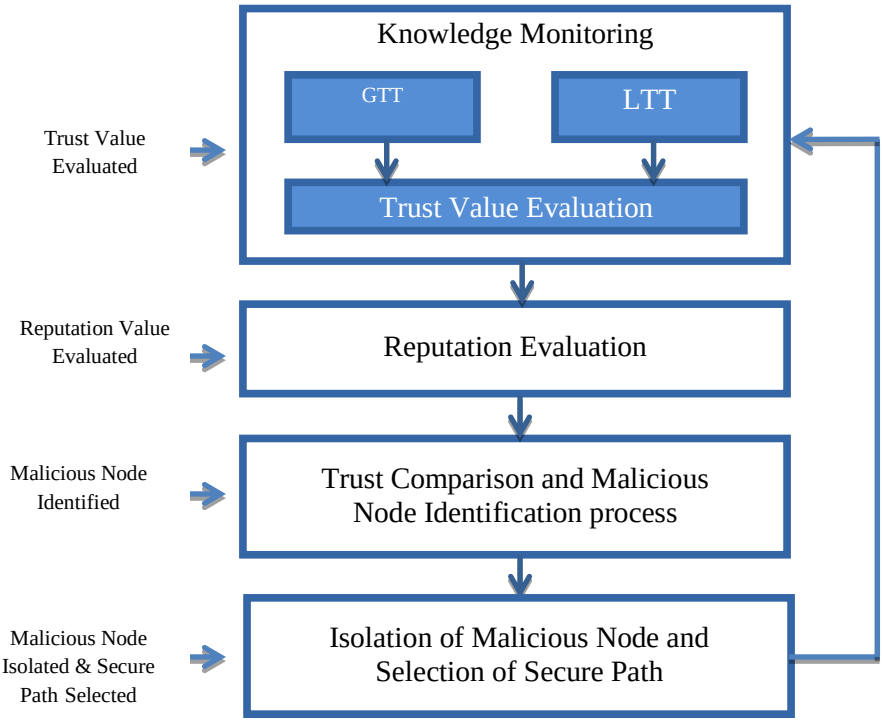


Fig.1 Proposed System
Autonomic Trust and Reputation Monitoring Scheme (ATRMS)

A. Trust Monitoring Scheme (TMS)

Trust monitoring scheme consists of Local trust values on the nodes and Global trust values on the RSUs to store trust values of the nodes present in the VANET network, it is also known as knowledge Monitoring as it provides us nodes knowledge. Local Trust Table (LTT) is the table where local observations are stored. This table contains the trust value of the neighbor nodes. Global Trust Table (GTT) is based on the LTT. Global Trust Table (GTT) is updated with trust values of all the nodes in the network. The GTT is stored on RSUs with the information of all the nodes participated in the network. For trust verification or updation nodes communicate with these RSUs for getting trust values of other network nodes.

Autonomic Trust and Reputation Monitoring Scheme (ATRMS) uses secure trust based data transfer protocol to establish trust relations between nodes in a VANET. Which allows self-adaptive monitoring mechanism thus, optimizing the network resources according to the underlying network's context? Each network's node is equipped by a TMS, ensuring trust knowledge monitoring in a distributed manner.

1. Local Trust Calculation

Local trust is calculated by observing local nodes. The node in the network gets information about the neighbor node trustworthiness based on number of packets it receives form that neighbor.

1) A packet is received by node 'i' from node 'j' it verifies if that packet was forwarded or generated by that node for checking its trust.
2) Only by observing the IP header that contains source address of the packet, node 'i' can get the information about origin of the packet.
3) Trustworthiness of node 'j' is evaluated by node 'i', taking into account amount of traffic generated by node 'j'. This ratio is the degree of trustworthiness in the link j-i.

$$R^{i}_{loc}(j) = \frac{aP^{i}_{f}(j)+bD^{i}_{f}(j)}{aP^{i}_{g}(j)+bD^{i}_{g}(j)} \qquad (1)$$

Where, P(j) node 'j' sent packet towards node i D(j) amount of data packets carry data generated by node 'j' is indicated by sub-index g and sub-index f indicates data forwarded by node 'j'. Different weights are indicated by 'a' and 'b'.

4) If amount of data forwarded by j is less than data generated by j then reputation of j is low otherwise reputation of j is high.
5) Reputation of the node increases only if the node forwards packets of another sender nodes.
6) GTT trust table is updated with the calculated trust values.
7) First step is repeated for all the nodes.

Local Trust Table (LTT) stores data generated by observations of local nodes and the trust values of all the nodes in the network.

$$localtrust = a * mobility + b * nbrs + c * datasent + d * oldtrust \quad (2)$$

Where, a, b, c & d - tuning constants that are determined during simulation. The sum of these constants equals 1
mobility - measured based on the number of changes in the one-hop neighborhood of a node
nbrs - the number of neighbors each node has
datasent - forwarded and generated packets sent by the observed node
oldtrust- the last trust value of the node; it presents the past activity of a node. Fig (3) shows a simple scenario. Node A directly observes the behavior of its one-hop neighbors B, C and D. It stores the values of the observed parameters in its local trust table.

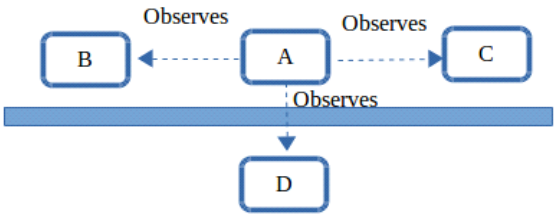


Figure3. A Simple Scenario

Local Trust Table (LTT) stores data generated by observations of local nodes in the network. The structure of LTT for node A is shown in Table 1. It includes entries for nodes B, C and D, and their behavior values. Node A computes a local trust value for each node based on the stored values as described in formula 1.

Table1: LTT for Node A

Node	Mobility	nbrs	data sent	old trust	local trust
B	0.5	0.8	0.34	1.3	2.94
C	0.4	0.6	0.56	1.64	3.2
D	0.3	0.2	0.18	1.05	1.73

2. Global Trust Calculation

The GTT is the main center from where all the nodes in the network communicate and exchanges information regarding neighbor node trustworthiness. GTT gets network nodes information from LTT and as and when required by the nodes in the network it exchanges its information. Local trust values are upended in the GTT which is in charge of exchanging information with other nodes. Based on the table LTT, Global Trust Table (GTT) is constructed which is successively completed by all network nodes trust values. Table 2 shows the structure of GTT for node A. Its structure is simple. It contains entries for all nodes in the network and their global trust values. B, C and D are direct neighbors for node A. E and F are not neighbors. So, GTT do not have local trust values for them. This table distributed among neighbors in order to compute and update the trust value for each node. If the node is a direct neighbor, its trust value is calculated using the local trust value and the remote information that is obtained from neighbor nodes. The new trust value that is stored in GTT will be:

$$newtrust = w_l * local_{trust} + w_r * remote \quad (3)$$

Where, w_l and w_r are weights and local trust has higher weight (w_l). For far nodes that are not neighbors for a node, the new trust value will be:

$$newtrust = remote \quad (4)$$

The remote information is:

$$\text{remote} = w_l * T_{est} + w_r * T_{rec} \quad (5)$$

where, Test is the value stored in GTT, and T_{rec} is the recommendation (local) received from a neighbor different from the owner of the table.

Table 2: GTT for Node A

Node	local $_{trust}$	T_{est}	T_{rec}	Global Trust
B	2.15	0.46	1.56	0.53
C	3.4	0.89	1.23	0.64
D	1.2	0.67	0.62	0.268
E	X	0.28	2.35	0.35
F	X	0.12	1.35	0.427

3. Node Trust Evaluation:

Each node creates its local trust table where it stores trust values of the neighbor nodes. The range for trust values are set to 0.5 to 2. A node with the best behavior is assigned with the highest trust value e. i. 2, the nodes detected with the malicious behavior is assigned with the trust value >0.5. The GTT are updated with the calculated trust values. Here, attacks related to the Link layer and physical layer are not considered. Instead, we have route trust values of the nodes and total number of nodes. Main advantage of the system is that malicious nodes are isolated from taking part in the network communication, as we consider only most trustworthy node in the network.

B. Reputation Evaluation

1. Global reputation can be evaluated using eq. (6).

$$R^i_{new}(j) = w_1 R^i_{loc}(j) + w_r \left(w_2 R^i_{est}(j) + w_3 R_{rec}(j) \right) \quad (6)$$

   Where, w1 + w r = 1 and w 2 + w 3 = 1 (adequate weights)
   Riest (j) – value of trust of node 'i' on node 'j'
   Rrec (j) – Reputation about 'j' received from other nodes.
2. New reputation trust value is stored in GTT.
3. All the nodes update their neighbor's trust values in GTT.
4. The updated GTT is exchanged between all the network nodes.

C. Malicious Node Identification Process

Step1. All network nodes trust value is initially set as 1.
Step2. After event generation, receiving node checks if event is genuine.
Step3. If yes updates its trust value otherwise check for the trust and reputation value count.
Step4. If average trust count is < 0.2 then the event is malicious.
Step5. If average trust count is in the range > 0.2 to <= 1 then the node is moderate trustworthy.
Step6. If average trust count is > 1 then the node is highly trustworthy.

Table 3: Updated GTT for Node A with Average Trust Value

Node	Local trust	T_{est}	T_{rec}	Global trust	Reputation Trust	Avg. Trust
B	2.15	0.46	156	0.53	1.5	1.02
C	3.4	0.89	123	0.64	2	1.49
D	1.2	0.67	0.62	0.268	1	063
E	X	0.28	2.35	0.35	0	0.18
F	X	0.12	1.35	0.427	0.5	0.47

D. Isolation of Malicious Nodes and Secure Path Selection

- **Isolation of Malicious Nodes:** The trust manager checks if the average trust count of the node is < 0.2 then that node is declared as malicious node and the malicious-intent message is broadcasted in the network, giving all the network nodes information about the malicious node. After malicious node detection any further message from the malicious node is ignored and that node is resisted taking part in further network communication.
- **Secure Path Selection:** A secure path selection process based on trust and reputation values are discussed below. Path manager checks the average trust value of the node in the route for malicious detection. If the

count is below the threshold level then path manager discards the route and search for the fresh new route. For secure path selection path manager performs following steps.

1. Source node broadcasts routing request message to its neighbors in order to find a route to destination node.
2. The neighbors of the source node forward the request to their neighbors if the trust evaluation on the source node passes its predefined threshold, and so on, until either the destination or an intermediate node with a "fresh enough" route to the destination is reached. And that node would like to accept the data transfer based on its trust evaluation.
3. If some nodes respond that they have fresh enough route to the destination node and would like to reserve some time slot for serving data transfer, the source node checks the trust evaluation using Trust Monitoring System (TMS) on the responded nodes.
4. Based on the trust evaluation result and hops of the routes, the source node selects one preferred route, which it believes the best.
5. After receiving the data packages, the destination node applies the same method above to reply the confirmation message if the source node requests it.

Features of ATRMS Algorithm

- Trust making based on server readings, decision making and previous trust value of the node
- Independent of the relative position of sender compared to the position of sending node
- Geo/ situation oriented reputation levels are used
- No cryptographic schemes are used
- Identification and Isolation of malicious node
- Protection against double-face attacks.

IV. Implementation And Handling Of Attack

The proposed algorithm handles four types of attacks, namely, false event generation, data modification, data dropping, and Double Face attack. The implementation and handling of the attacks is as described below.

- False event generation is a type of attack in which a vehicle generates information about an event that actually does not exists. This can be detected with the help of sensors. If a node in the detection range of an event has no information about the event then the event is definitely not genuine. Thus a false event generation can be easily detected.
- Data modification is a type of attack in which a vehicle purposely modifies the type of event that is a traffic jam to an accident or vice versa. For this a vehicle changes the type of event field in the data packet. In our algorithm an event is taken to be genuine only if either a required number of nodes generate that information or the information is received from a required number of trusted nodes such that a minimum threshold is exceeded. This feature helps to detect data modification.
- Data dropping is a type of attack in which a vehicle does not forward the information it is supposed to forward. In our algorithm neighbor monitoring is a continuous feature in which the nodes simultaneously monitor their neighbor nodes. Thus, if a node has received a packet but is not forwarding it the neighbor nodes can safely assume it to be a data dropping node.
- Double Face Attack is a type of attack in which double-face attacker node which acts as a source node makes use of network but starts dropping received packets after a period of time of normal behavior. These attacks cannot be detected based on local information. Hence, in order to enforce the knowledge a node has about a neighbor global trust is also considered. Trust estimation approach is used to handle double face attacks.

V. Proposed System Performance

The IEEE 802.11 distributed coordination function (DCF) is used as medium access control (MAC) protocol. In the simulation experiments, a network with 1000m x 800m area and 20, 60 and 100 mobile nodes was simulated. The simulation time is 1000 seconds. The mobile nodes move within the network space according to the Random Waypoint model. The communication patterns used are 6 Constants Bit Rate (CBR) connections with a data rate of 10 packets per second. The total number of nodes (nn) placed randomly in this area is 20, 30 or 50 nodes, characterizing networks with different densities. 10% of double-face attacker nodes are chosen randomly from the total number of nodes in the beginning of each simulation. Those malicious nodes drop or forward packets. A double-face attacker node is a source node which makes use of network but starts dropping received packets after a period of time of normal behavior. The data traffic used is CBR (Constant Bit Ratio) with a number of connections (nc) equal to 5 or 10 defined randomly. Each source node generates 4 packets/sec with a packet size of 512 bytes. The total simulated time was 100 seconds and each plotted point is an average of 10 simulations.

For evaluating the performance of the proposed system three commonly used metrics are used Packet Drop Rate (PDR), percentage of malicious nodes detected and control packets sent. From Fig (4) we can see that, control packets sent

after detection of malicious nodes increases with the number of malicious nodes increase in the network. This is because with detection of greater number of malicious nodes more control packets is to be generated to notify the network about the malicious event.

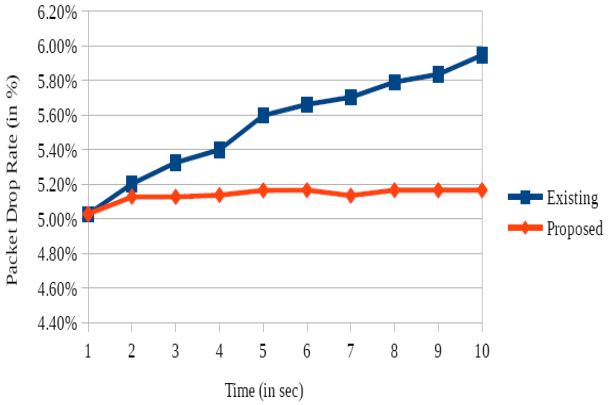


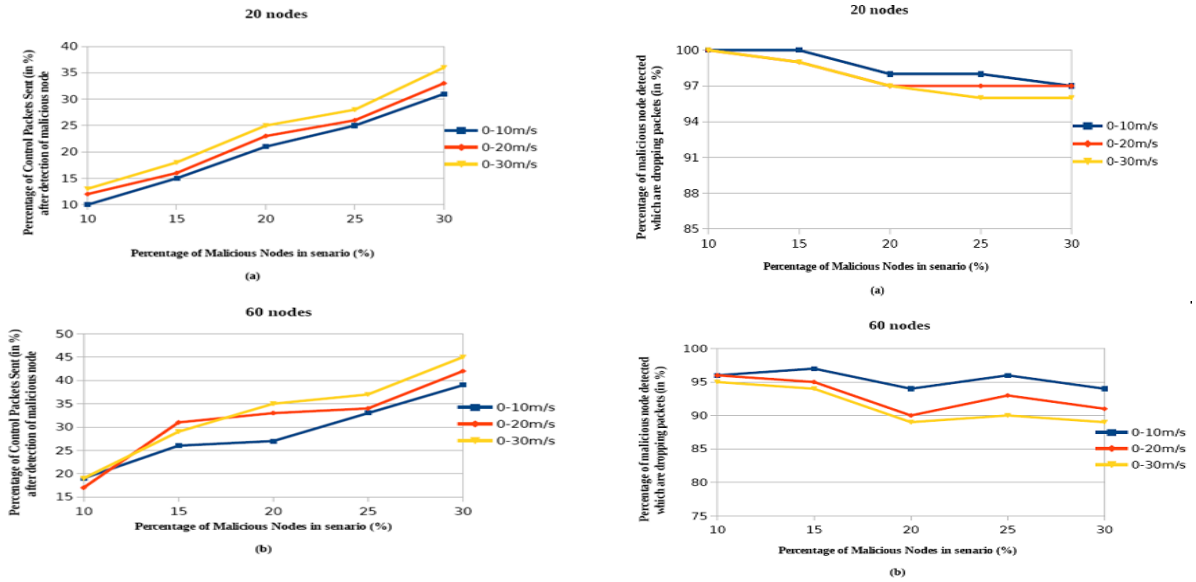
Figure 4. Comparison of Existing and Proposed Scheme (Packet Drop Rate)

Three different cases have been simulated with different number of nodes.

1) No. of nodes = 20 Fig. 5.2 and 5.3 show different cases where the speed of a node is varying between 0-10 m/s, 0-20 m/s and 0-30 m/s. Number of events taking place in this case are 5.

Analysis: In this case, there are not many nodes in detection range of each other. This means that if a node performs a malicious activity, the probability that some other node may detect it, is not very high. Due to this, it can be seen from Fig. 5.2, that the variation in the number of malicious nodes detected in the network, is very high. As the number of malicious nodes in the network increases, the probability that a node is in the detection range of malicious node increases and also the probability of many malicious nodes in the detection range of each other also increases. This means that in the first case, more number of malicious nodes should be detected and in the latter case, lesser number of nodes should be detected as malicious.

2) No. of nodes = 60 Number of events taking place in the network here are 15.
Analysis: In this case, the probability of occurrence of nodes in the detection range of a malicious node increases further. So an overall improvement in the percentage of nodes detected as malicious over the previous case can be seen. Here more number of malicious nodes is detected with lower maximum speed than nodes with greater maximum speed.
3) No. of nodes = 100 Number of events taking place in the network here are 25.
Analysis: In this case, the detection percentage decreased for all speeds. Here it can be seen that the number of control packets transmitted in the network increased. The reason is that, in this case more number of nodes is in detection range of each other. So, more number of nodes can detect a malicious activity. Thus, more nodes forward the same information. In this case, the number of events is more; therefore, more control packets are generated.



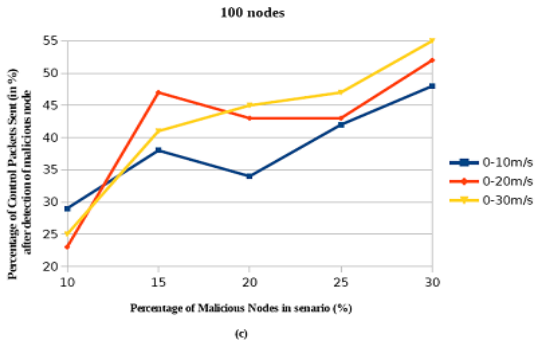


Figure (5) Percentage of Control Packets sent after detection of malicious node for 20, 60, and 100 nodes, respectively. Average of control packets sent after detection of malicious nodes (a) 20 nodes is 221333, (b) 60 nodes is 31.667 and (c) 100 nodes is 40.80.

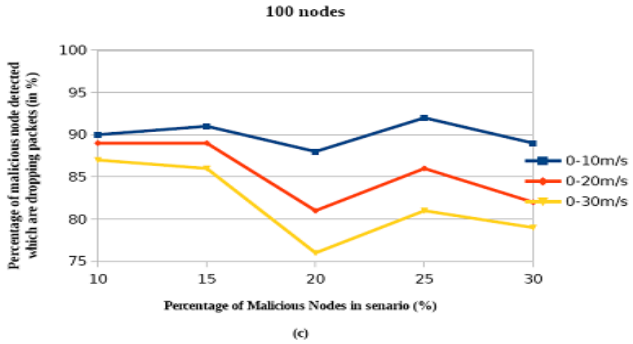


Figure (6) Percentage of malicious node detected which are dropping packets for 20, 60, and 100 nodes, respectively. Average of malicious node detected for (a) 20 nodes is 98.06667, (b) 60 nodes is 93.26667, (c) 100 nodes is 85.93333.

Average of control packets sent after detection of malicious nodes (a) 20 nodes is 22.333, (b) 60 nodes is 31.667 and (c) 100 nodes is 40.80. Control packets sent after detection of malicious nodes increases with the number of malicious nodes increase in the network. This is because with detection of greater number of malicious nodes more control packets is to be generated to notify the network about the malicious event.

Average of malicious node detected for (a) 20 nodes is 98.06667, (b) 60 nodes is 93.26667, (c) 100 nodes is 85.93333. The average of malicious nodes detected for various speed shows that with lower speed, detection rate is greater and for the higher speed detection rate goes on decreasing as topology changes rapidly. For higher density network with high speed detection rate is lower.

VI. Conclusion And Future Work

Proposed system Autonomic Trust and Reputation Monitoring Scheme (ATRMS) is based on autonomic principles and a trust and reputation based routing protocol for enhancing trust management and security in VANETs. The proposed scheme provides robust communication in the accident related case. It is a secured algorithm which reduces the impact of illusion and double face attack. The proposed system provides up-to- date trust knowledge throughout the network with a minimum monitoring overhead, the system also detects and isolates malicious nodes in the network. The perfect security in VANETs is very hard to achieve but using the proposed system threats can be greatly reduced. The proposed algorithm provides less broadcasting rate, less packet drop rate, and high packet delivery ratio compared to the existing system. As in the system node forwards the packets intelligently by checking sender nodes trustworthiness and taking autonomic decisions using the network information and not forwarding the messages as it received from the nodes, hence it reduces broadcast overhead and makes the system more efficient. Most of the security based systems only detects the malicious nodes, but the proposed system not only detects but also isolates the malicious nodes from taking part in the network communication.

The ATMS framework which was presented in [2] was developed for MANET network. In the proposed scheme the ATMS framework was modified using trust based routing protocol to enable the scheme to be used for VANET networks also. The conclusion is that the proposed system can be used as a generalized system for MANET and VANET wireless communication networks. In future work, plan is to extend the system to provide information to a particular region that is geocasting. Study the possible use of vehicle to vehicle communication without using any infrastructure for the purpose of providing traffic information. Also plan is to study other applications of VANETs such as automatic toll collection, location-based services and entertainment.

References

[1]. Dhurandher, S.K., Obaidat, M.S., Jaiswal, A., Tiwari, A. and Tyagi, A., 2014. Vehicular security through reputation and plausibility checks. Systems Journal, IEEE, 8(2), pp.384-394.

[2]. Movahedi, Z., Nogueira, M. and Pujolle, G., 2012, April. An autonomic knowledge monitoring scheme for trust management on mobile ad hoc networks. In Wireless Communications and Networking Conference (WCNC), 2012 IEEE (pp. 1898-1903). IEEE.

[3]. Dotzer, F., Fischer, L. and Magiera, P., 2005, June. Vars: A vehicle ad-hoc network reputation system. In World of Wireless Mobile and Multimedia Networks, 2005. WoWMoM 2005. Sixth IEEE International Symposium on a (pp. 454-456). IEEE.

[4]. Chen, C., Zhang, J., Cohen, R. and Ho, P.H., 2010, August. A trust modeling framework for message propagation and evaluation in VANETs. In Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on (pp. 1-8). IEEE.

[5]. Lu, R., Lin, X., Zhu, H., Ho, P.H. and Shen, X., 2008, April. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications. In INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE.

[6]. Al Otaibi, S. and Siewe, F., 2009, December. Secure Routing Protocol base on secure path in ad hoc wireless networks. In Computer Science- Technology and Applications, 2009. IFCSTA'09. International Forum on (Vol. 2, pp. 46-53). IEEE.

[7]. Fonseca, E. and Festag, A., 2006. A survey of existing approaches for secure ad hoc routing and their applicability to VANETS. NEC network laboratories, 28, pp.1-28.