International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.07, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

# A SURVEY ON SECURITY AND TRUST REQUIREMENTS AND MANAGEMENT IN VANET

**Bonish Koirala[1], Shrikant S. Tangade[2], Sunilkumar S. Manvi[3]**

*[1,2] School of Electronics and Communication Engineering, REVA University, (India)*

*[3] School of Computer Science and Engineering, REVA University, (India)*

## ABSTRACT

*Vehicular Ad hoc Network is an application of intelligent transport system which focuses on the aspect of vehicles being able to communicate with each other and transmit necessary road information. As technology advanced to implementation of wireless ad hoc networks, it has been a field of interest for the past few years to many researchers. This is mainly because of the diverse nature of the vehicles in VANET to which solutions of other ad hoc networks cannot be implemented. This paper first focuses on the similarities and differences of VANET with other networks and how they contribute to the unique security requirements and attacks in VANET. Then it gives a brief introduction to trust requirements and management models that provide solution to securing communication in VANET environment. A few points are included which reflects the considerations that should be kept in mind while developing a trust model. With the help of this paper, researchers can have more exposure to the current scenario of security and trust in VANET.*

## I. INTRODUCTION

Vehicular networks are highly dynamic [1]. The network topology changes frequently while the mobility of the nodes are geographically constraint. Due to these reasons, VANETs have the risk of security threats and attacks that are not avoidable by the security solutions applicable in other wireless ad hoc networks with high efficiency. Most of the solutions proposed to protect VANET from attacks include mostly cryptography. This includes digital certificates and signatures, encryption key exchange, trustable third parties and central authorities. Cryptography is an efficient solution to protect the network from external attacks. But cryptography cannot provide security when an authorized vehicle that is registered in the network turns malicious or selfish [3]. In this case, trust management is agood alternativefor limitations of cryptography to protect the network from internal attacks.

Trust is a level of confidence on the basis of which a node believes in the information sent by another node. It is the foundation on which communication between two nodes can happen in a secure manner. It is a necessary consideration to realize whether or not the information exchanged between nodes is reliable [2]. Trust can also be thought of as the reputation of a node where the other nodes can immediately believe the reputable node in a network without any involvement of a third party.

Trust between two nearby vehicles remains for a short duration of time due to the high mobility and dynamic nature of the VANET. It is established based on different factors such as historical interactions that can be both direct and indirect, past experiences with the node, level of reputation of a node within the network, recommendations from nearby nodes, etc. Trust Evaluation is based on all of these factors and it is done frequently in order to keep the trust value of each node updated [4].

*Organization of this paper:* Section II provides the different unique characteristics of the nodes in the vehicular environment. Section III gives an insight to security requirements and attacks in VANET. Section IV describes specific requirements that a trust management scheme should fulfilwhile Section V classifies and describes the trust management models that are already proposed accordingly. Section VI includes additional considerations that should be kept in mind while designing a trust model. Then, the conclusion of the survey is provided at Section VII.

## II. CHARACTERISTICS OF VANET

Below a list of VANET characteristics that clearly specifies the similarities and differences of VANET with other wireless ad hoc networks:

2.1. High Mobility: A VANET consist of numerous vehicles each having their own speed and acceleration. The speed can differ according to the speed limit rule, driving area and the density of vehicles in the road. For the vehicles with high speed, location of a node is difficult to predict [14].

2.2.Rapidly Changing Network Topology: The objective of movement of vehicles in a VANET is not to maintain the network topology. It depends on the source and destination of the passengers and the speed of the vehicles. Due to this reason, node movements are unpredictable in VANET [13]. This is the basis which makes a VANET highly dynamic.

2.3. Unbounded Network Size: Vehicular Network is not limited by the geographical area. The network in scalable such that it can be increased from a city size to a whole country [13]. The challenge in this would be the use of alternative wireless access technologies in different scenarios such as urban and rural areas.

2.4. Frequent Exchange of Information: The VANET is an ad hoc network. The nodes rely on other vehicles and road side units for transmission and reception of alert messages. So, there is a frequent exchange of information between the nodes in the network.

2.5. Bandwidth Limitation: 75 MHz of spectrum in the 5.9 GHz frequency band has been allocated for DSRC applications by the FCC [15]. So, the bandwidth for communication between nodes in VANET is limited.

2.6. Time Critical: Highly mobile nodes require information that are accurate in time. As vehicles carry people, it is very important that the nodes in VANET get highly approximate time reference. Failure in this can result to grave dangers and accident.

2.7. Wireless Communication: An obvious characteristic is that nodes transfer information wirelessly. Wired communications are too impractical for dynamic networks like VANET. But along with wireless communications comes the security risks and vulnerabilities associated with it. Due to the physical support of wired communication, it is regarded much safer than wireless networks.

2.8. Energy, Storage and Computing: One of the best characteristics of VANET is that it has very high energy efficiency, more storage capability and better computing power. This is because the nodes are the vehicles and the RSU themselves which have no problems with these factors.

2.9. Protection against physical vulnerabilities: Physically compromising the vehicles is much more difficult in VANET than in any other ad hoc networks. So, the OBU of the vehicles have no problem against external physical attacks.

## III. VANET SECURITY

Securing communication in VANET is a major issue. Importance of security in VANET is further increased by the fact that VANET is dynamic in nature and a poor VANET architecture can leave the network vulnerable to various type of attacks which leads to compromising the passenger safety [10]. Security solutions implemented for VANET should ensure message authentication and information integrity. This means that whenever a node receives a message, he needs to be sure that it is from an authenticated source and in not modified or amended with malicious intent during transmission [2]. These solutions also need to integrate the feature that privacy of the nodes is safe and is not compromised by another malicious node using the information in the message.

### 3.1. Security Requirements

The basic security requirements in a VANET environment is given below:-

3.1.1. Confidentiality: In VANET environment, the information exchanged in form of messages from one node to another is to be encrypted by the use of digital keys and signature. Confidential information exchange can be ensured mainly by the use of cryptography rather than trust [3] as the information should be readable and usable by only the designated source and destination.

3.1.2. Integrity: Integrity refers that the messages are not modified mid-way while transmitting from source to destination. If the message is not encrypted using proper encryption standards or the malicious node has sufficient information about the encryption, then the integrity of the message can be compromised. Security solutions must employ a robust encryption mechanism to ensure integrity.

3.1.3. Availability: The network functionality and service should be available for the users to send and receive messages without delay. Malicious users are primarily launching an attack such as the DoS on the network to deny the users from basic VANET services.

3.1.4. Privacy: Since the peer-to-peer communication is based on the position of the nodes in the network, there is a high probability that the malicious node might be packet sniffing to gain access to the personal information of a node. Security solutions must consider the aspect that although identification and positioning of a node is important for transmission of message, privacy of the node must also be secured.

3.1.5. Authentication: Authentication refers to the identification of the message sender whether it is a genuine or an unknown node. An authentication scheme must be employed in the security solution that if a sender wants to provide information in the network it must be identified by the network administrator to do so. Authentication and Privacy comes in conflict because of the opposite nature of these requirements. So, security solutions must be able to handle this conflict.

3.1.6. Non Repudiation: Non Repudiation is the justification that an action performed by a node is indeed its own and not confused with some other node. It is regarded as matching of a node's identity with its action [10].

3.1.7. Access Control: Access Control is needed in the vehicular network such that vehicles abide by the network rule and access the service only when required. As network resources such as bandwidth is limited and the number of vehicles in an area can be very huge, it is important to provide some mechanism that nodes use the service in a controlled manner [6].

## 3.2. Security Attacks

Given below is a briefly detailed list of the various type of attacks that could be launched to compromise the security of the vehicular network.

3.2.1.Denial of Service: Denial of service is the type of attack where the service provider is overloaded by the attacker. The attacker continuously feeds the service provider with fake requests which seem to the provider as a legit one [5]. Due to this, the legitimate service consumer will not get any response from the service provider and its request gets dropped after a certain time. In VANET, DoS attacks are dangerous because even a small delay in communication can lead to fatal accidents.

3.2.2. Distributed Denial of Service: DDoS is similar to DoS attack in application but in this case the attack is launched by multiple malicious vehicles. The targeted vehicle or service gets overwhelmed by the fake request or the malicious nodes. It may be highly improbable considering that multiple malicious nodes do not work in unison but still an effective attack strategy that can exhaust the service provider and the network.

3.2.3. Sybil Attack: When the attacker produces multiple identities to conceal his own identity in the network, then the attack is termed as Sybil Attack. It is possible if the malicious node has gained enough information about the identities of the nodes in the network or the procedure of pseudonym generation by authenticated nodes. This can be used to launch other attacks in the network using fake identities or make the network believe there are multiple non existing vehicles in the network [10].

3.2.4. Wormhole Attack: In this type of attack, 2 or more malicious nodes work in unison in order to create a wormhole also known as a tunnel [10]. When a message is received by a malicious node, it is routed through the tunnel to the other side of the network and broadcasted there by the other malicious attacker. It is a critical attack that can cause much harm if the message that is tunnelled is time/position sensitive.

3.2.5.Black hole Attack: It is an attack which creates the illusion to the nearby nodes that the best path of routing is through the attacker node. The illusion may be based on the shortest path or the most secure path for routing. After the attacker receives message packets from the other nodes, it drops all the packet thus creating a black hole scenario for the safety messages to be sucked in.

3.2.6.Grey hole Attack: It is similar to black hole attack but instead of dropping all the packets, the attacker selectively drops only some packet. While this may seem less dangerous than black hole attack, it is not so. Messages are sent in form of packets and each packet contains partial content of the complete information. If some packets are dropped, it hinders with the message integrity and the receiver may receive false and confusing information.

3.2.7. Application Attack: VANET has many application such as safety messages distribution, finding destination location, social platform for vehicular communication, etc. Application attack simply refers to when the attacker mostly targets the application domain of VANET such as altering the information shown by the application to the user which makes the driver trust or get distracted based on a false notification.

3.2.8. Timing Attack: This type of attack targets the time factor of the messages. VANET is extremely sensitive with time. This attack introduces extra delay in the message to be relayed so that the message loses its importance after itsTTL (Time to Live) and gets dropped. So even legit messages will be dropped as irrelevant information.

3.2.9. Replay attack:When a same message is transmitted over and over again in the network, it is known as a replay attack. This attack can be avoided by the use of sequence numbers and timestamps [1].

3.2.10. ID Disclosure Attack: In this attack, the targeted node is constantly monitored to know its current position. This type of attack is usually done by the vehicle manufacturing company and rental organizations to keep track of its vehicles [1]. It may also be done by a malicious node if it has sufficient private information about the vehicle.

3.2.11. Eavesdropping Attack: Eavesdropping attack is a passive attack in the network as it does not involve any disruption in communication. In this attack, the attacker silently observes and monitor the activities of the target node [5], analysing its broadcasted message. This attack is used to gain enough information about the target node and finally deploy a fatal attack at the correct time.

3.2.12. Masquerading Attack: In this attack, the attacker masks itself as another vehicle in order to seem like a regular and authenticated node of the network. Using this fake identity, it can easily send false information to other normal nodes in the network and drive them to trust it.

3.2.13. Global Positioning System (GPS) Spoofing: GPS spoofing is a form of faking your own position to conceal the location of the node. The attacker basically provides false location information along with the message to different nodes [5]. It remains hidden as it cannot be tracked by using the location information.

3.2.14. Prank Attack: In this type of attack, the attacker sends different alternative messages to different vehicles. If the receiver vehicles trust and accept the messages, their actions will come in conflict with each other and thus cause accident [5].

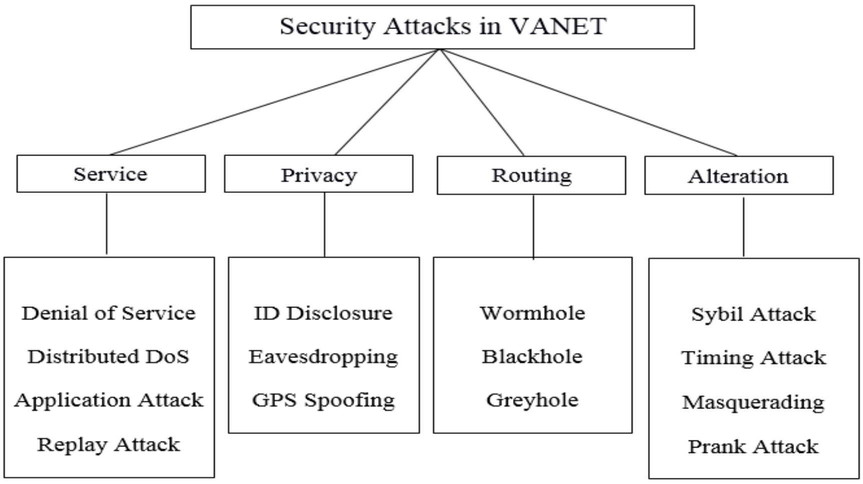

**Fig.1: Classification of attacks based on their nature**

## IV. TRUST REQUIREMENTS FOR VANET

Trust is an alternative to cryptography for ensuring security in VANET. In trust-based security the receiver vehicle is to perform corresponding action based on the message sent by the receiver vehicle. Receiver node must be capable of checking the trustworthiness of the message before taking any action [4]. So, any trust management solution designed to enhance security requires a few set of factors and parameters to evaluate the authenticity and validity of the node and the message. Following are a few requirements for designing Trust Model.

4.1. Decentralized: Decentralization refers to an environment where there is no central authority for managing all the nodes. Instead the work of the CA is distributed to several other nodes. Trust Model should consider the fact of ad hoc nature of VANET and that trust evaluation happens in a decentralized manner. Each node must have the ability to evaluate trustworthiness of node and its message. Mostly data-oriented trust models [20][21] are decentralized. Proposals such as [24][25] are cluster-based whereas [19][23] still rely on central authority for some specific task such as database management.

4.2. Scalable: Trust models should be designed to be adapting to the varying change in density of the network. It should be capable of gather, process and act upon a large amount of information when abundant trusted peers are available in a very busy network scenario. It should also be capable to keep up the computation with limited information when enough peers are around. [19] has specified scalability in terms of the vehicle density as a crucial factor in trust management.

4.3. Privacy: Along with joining in the network comes the matter of privacy. As discussed earlier, privacy is a more pressing issue in case on VANET because it is in conflict with authenticity. Privacy should be kept secure of not only the receiver but also the sender as malicious node might be sniffing packets sent by a certain node to launch an attack later. While designing a trust management scheme, consideration should be taken on how to build a strong trust between peers such that they have confidence that their privacy won’t be invaded.

4.4. Robustness: As discussed earlier, there are a number of attacks that can be launched in a number of ways within the network. A trust management scheme should be robust enough to secure the network against maximum of these attacks. [24][26] use an intrusion detection method that is specifically focused on identifying and preventing security attacks in the network.

4.5. Justifiable: Trust Models should be equal to all the nodes in the network. As long as there is no evidence of a node performing a certain malicious activity, it should not be charged with punishment. On the contrary, a node should be charged with punishment if it has carried out malicious attacks in the network regardless of the reputation of the node [8]. It should also be capable of identifying false positives and false negatives so that any innocent node is not punished. [16] provides a justifiable scheme that employs cost and reward to trustful nodes in the network respectively.

4.6. Attacker unawareness:The attacker should be kept ignorant that it is being subjected to punishment while it is launching an attack. If it gets aware that it is being punished, it may change its identity to start anew from a neutral trust value escaping the punishment [8].

4.7. Event/Task and Location/Time Specific:Different form of events can take place in a vehicular environment which generates different types of alerts and information message. Based on the alert, a receiver vehicle is to perform a certain action immediately. The alert may also have less importance to which a little amount of delay is tolerable. Trust model should be able to categorize the types of event and their alert message so as to define the weight of these alert messages. Similarly, the model should also consider the location and timestamp of the event. The nodes nearer to the event or that has happened most recently should give more weightage to the alert messages than those nodes which are far away from the event or the timestamp was created a long time ago. Messages format in [17][20][21] sent location and time information along with the alert for the receiver to analyse.

4.8. Integrated Confidence:Information that is incomplete introduces much uncertainty while evaluating the trust of a peer. While evaluating the trust, a certain level of confidence should exist such that the information gathered is thought to be true. Confidence can be thought of as within a range of [0, 1] [11]. It increases as more evidence contributing to the validation of a certain parameter to calculate trust is increased. Most papers [16][17][18][19][20][22][25] have used feedback and opinion collection from peer nodes to build confidence on the message.

4.9. System security: Trust models assume that the peers in a network can be identified with their own ID. So the system should provide a secure way for the peers to authenticate themselves. Digital Signatures, PKI cryptography schemes can be used to register a node in the network. Information exchange, node authentication, message validity can be ensured using cryptographic schemes so that the system is safe from malicious nodes.[23][25] have employed authentication schemes such each vehicle is identifiable within the network.

## V. TRUST MANAGEMENT IN VANET

Trust Management Schemes are proposed in order to fill the security gaps that are unable to fill by cryptography. Cryptography is no doubt effective against external attacks. But in case of internal attacks, trust establishment and management is the best way to secure peer to peer communication [3]. A trust management model provides the nodes with confidence to believe that the information they are sharing with each other are valid and taking part in the network will not harm them in any way if they are honestly working as a legitimate node of the network. Trust was mainly employed in VANET so that peers can clarify whether or not to believe another peer of the network.

Some believe that the trust evaluation of a node can be taken in consideration in order to manage trust, while others believe that it is actually the data and information regarding an event that is flowing around the network that is to be trusted and the identity of the sender need not be associated with it [8]. Trust management models are mainly categorized into 3 different parts according to what the trust models are entrusting in.

1) Entity Oriented Trust Model

2) Data Oriented Trust Model

3) Hybrid Trust Model

Entity Oriented trust models focus on the trust value evaluated of a node whereas Data Oriented models are based on the trust of the data in the network. Hybrid models are just a combination of both of these models where node and data trust both are considered and merged with other technologies that can be well applied in dynamic scenarios of VANET.

### 5.1.Entity Oriented Trust Models

The entity oriented model are based on the activities of a node. It considers the fact that if a node is not performing any malicious activities his trust level will be high in a network whereas malicious nodes will have low trust level. The trust evaluation of the nodes are based on the parameters such as old trust level, number and weightage of valid messages sent, number and weightage of attacks launched, history of interactions, reputation in the network, etc.

Khan et al [23] proposed a cluster based method to evaluate the trust of nodes. A list of verifiers are chosen based on load, distrust value and distance which are used as decision parameter for trust. The verifiers monitor the behaviour of a newly entered node in the cluster. If an abnormal behaviour is found, it is reported to the cluster head which then calculates a new distrust value for the node and informs it to nearby nodes. If the distrust value of a node exceeds the threshold value, it is blacklisted. White list and Black list are maintained to classify trusted and untrusted nodes respectively.

Hadaddou et al [16] proposed a credit based system where each node gets a certain amount of credit value when it is first connected to the network. Whenever a source node has to send a message it associates a certain amount of credit along with the message as a guarantee of trust that the message is valid. The credit amount is based on how relevant is the information and how is the source's reputation with its peers. If the information received is found valid, then the source is rewarded with certain amount of credit. A node is excluded from the network if the credit amount reaches zero.

Yang et al [17] has proposed a technique which uses similarity mining based on Euclidean distance and evaluation of reputation. In his work, he has presented similarity of two factors i.e. Message Similarity and Vehicle Similarity. Message similarity is based on the event and location of alert included in the message whereas Vehicle Similarity depends upon Speed, Direction and Reputation. It is assumed that RSU and service vehicle such as police, ambulance have usually high reputation. These reputation are used as weights to calculate trust of the node and is constantly updated. Reputation information may be from direct experience or by recommendation from neighbors.

Jesudoss et al [25] has proposed a payment punishment scheme having a cluster based mechanism where cluster head is will be elected as the one with greater weights. The runner-up of the election is chosen as Auxillary CH. This can be used for making routing decision and building a trust environment. After the election has been completed, a certain reputation value is given to each participating nodes which determines the trustworthiness of these nodes. Reputation can also be increased by forwarding messages and reporting misbehaviour of other relay nodes by monitoring them as watchdogs. Reputation table is continuously updated and broadcasted to all the nodes in the cluster.

### 5.2. Data Oriented Trust Models

Data oriented trust models are based on the information and data rather than the sender itself. It considers the trustworthiness of the data by checking the authenticity, accuracy and validity of the information sent by other nodes.

Gurung et al [20] has proposed a message and route similarity based method where each vehicle has the capability of evaluating trust of message without use of central authority. Each message has a trust value that denotes the possibility that the message is true. This trust is evaluated on the basis of its contents and the route it took to reach to the receiver. In case two message claim having the same origin but different content, the receiver trusts the one with highest trust value.

Shaikh and Alzahrani [21] have proposed a V2V communication based trust evaluation and considered the fact that VANET are not limited in terms of memory, power, computation etc. Confidence is calculated for messages received by a vehicle and trust is evaluated for the message. The method consist of 3 stages of message trust evaluation. In the first phase, a confidence measure is generated for each messages that is sent from a unique sender. The measure depends upon closeness and verification of location and time. Location information gives message reliability whereas time information gives message freshness. In the second phase, trust values are calculated for each unique message that is related to a unique event. In the third phase, the message having highest trust value is accepted.

Golle et al [22] proposed a sensor driven method where the each node can tell the other nodes apart. Each node will build its own model of the VANET which consist of all the possible information it has on the VANET. When a new data is received, the node will gather explanations for the data. The explanations are then scored based on the level of consistency with its own model of the VANET and finally the explanation with the highest score is accepted. The proposal is built on considerations that malicious nodes are usually a few in number and shows disagreement in data it has sent.

### 5.3. Hybrid Trust Models

Hybrid trust models considers both the trustworthiness of the node and the data. It can be thought of as a two level trust evaluation model where the trustworthiness of the node is computed first and then the result is used to evaluate the authenticity of the data. Since these trust models take both into account, a considerable amount of fast computation is required.

Zhang et al [18] has proposed a method to evaluate and propagate a message based on the trust. In this model, each node has the capability of evaluating trust based on the opinions gathered from neighbour nodes. Each message received will be associated with a quality which is developed based on a trust value. This trust value is computed using other peers opinion on the message. During propagation, the opinions are also attached with it. Any receiver will then just have to check the list of opinion to make a decision on whether to trust or not to trust the message. High quality messages will be propagated the farthest whereas low quality messages that could be sent by malicious nodes are controlled to a local cluster.

Marmol and Perez [19] has proposed a similar technique of trusting a message based on other peers. In this case, the reputation of the message sender is taken based on 3 factors which are, direct experience, recommendation from peers and recommendation from central authority. The reputation will classify the sender in 3 fuzzy sets. Then the decision on the message will be made (to discard the message, accept but not forward or accept and forward) based on which set the message sender lies in. More the reputation of the sender, more the importance of the message. The central authority will manage a database on each of the malicious vehicles.

Sedjelmaci et al [24] proposed an intrusion detection mechanism that is mostly deviated towards detecting and preventing security attacks from malicious nodes. The architecture is cluster-based and the leader of the cluster is selected based on the mobility of a node and its trust level. It uses 3 intrusion detection systems i.e. detection at a local cluster level that is rule based, at a global level consisting of cluster heads that uses hybrid detection and decision making at a global level.

Kumar and Chilamkurti [26] proposed another intrusion detection system that employs a Learning Automata to detect different states such as density, mobility and direction of the vehicles in the network. State transition is represented by a Markov chain model and is dependent upon those vehicular parameters. A mobility aware authentication mechanism which verifies the authenticity of the nodes in the environment. For each action, a collaborative trust index is computed whose value increases or decreases according to success or failure of the action. If the values in the CTI goes below a certain amount, it represents a malicious activity.

## VI. ADDITIONAL CONSIDERATIONS FOR TRUST MANAGEMENT

### 6.1. Any node can go malicious

In a vehicular scenario, a lot of different type of vehicles cross through the same path every day. Even the most reputable nodes in the network such as police, ambulance has equal possibility of going malicious and launching an attack in the network. This can be due to attacker hacking in the reputable nodes with a big motive in mind or willingly with mischievous intent by the users of the nodes themselves. This also gives reason why a trust model should be justifiable and should establish reward and punishment equally to all the nodes

### 6.2. 100% trust is practically infeasible

Though trust of each node can be computed using mathematical equations, a full trust in each node can be established only theoretically. Practically, just like in a real life scenario, even the highest reputable nodes have equal probability of going malicious as discussed earlier. This probability makes it infeasible to fully trust any node in the network.

### 6.3. Unique trust view of each node

The authority of making decision on whether to trust or not to trust a message sent by a peer should be in the receiver nodes themselves. A user should be able to calibrate the trust settings in his vehicle so that the node can be safe while entering an unfamiliar network with high security threat.

### 6.4. Need for a third party

Vehicular networks are ad hoc by nature. The use of third party in a Vehicular network scenario is a topic of major discussion. On one hand, use of a third party such as a cluster head or central authority can release computation burden from the nodes which rarely remain in the network but introduces much delay in the network as message propagation and processing will take a considerable amount of time. On the other hand, in a fully ad hoc network, a node needs to gain enough confidence in a message to judge it as valid. This can be done by collecting opinion about the node or the message from peers. But there is no guarantee that the opinions themselves are also valid.

### 6.5. Nodes are not always mobile

Most of the proposals take the consideration that only the RSU units are stable and vehicles are always mobile. This is not always true. A vehicle that belongs within the network (for eg:-home parking spots, parking lots, personal vehicles in office environment, government vehicles when not in use such as police, ambulance, etc.) will stay in the network for a very long time. This can contribute to better stability of the network.

## VII. CONCLUSION

This paper provides an insight to the different characteristics of VANET that needs to be considered such as high mobility, rapid topology change, unpredictability etc. and how these factors makes it different from the rest of the ad hoc network domain. It presents the different security requirements and attacks that are unique to VANET environment. While both cryptography and trust management are required to keep the network secure, this paper focuses on trust requirements and proposals contributing to trust management. Real cases such as any node going malicious and presence of some stable vehicles in the network are also included as considerations for trust schemes.

Trust management has the ability to classify a malicious vehicle from the rest of the network. Different trust management schemes have been proposed in order to maintain trust between vehicles within the network so that vehicles can exchange information quickly and reliably. A set of trust requirements need to be fulfilled whenever a new trust based scheme is proposed. The trust management schemes that have been proposed so far are only limited in simulation and have not been implemented so far in real time scenario.

## REFERENCES

[1] L Sharma, S K Bharti & D K Yadav, *" Vehicular Ad Hoc Networks (VANETs): A Survey on Security issues and challenges", International Conference on Advances in Computational Techniques and Research Practices, pg 130-135, Vol. 6, Special Issue 2*, February 2017.

[2] D. Soni, R. Gupta & V.Namdeo*,"A Review on Trust Management in VANET", International Journal of Advanced Research in Computer and Communication Engineering, pg 30-34, Vol. 6, Issue 6*, June 2017.

[3] C Kerrache, C T Calafate, J Cano, N Lagraa & Pietro*," Trust Management for Vehicular Networks: An Adversary-Oriented Overview ",IEEE ACCESS.2016, pg 9293-9307, vol 4*, December 2016.

[4] F Ahmad, J Hall , A Adnane & V. N. L. Franqueira, *"Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-hoc Network", 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pg 44-52*, June 2017.

[5] A. N. Upadhyaya, J.S. Shah, *" Attacks on VANET Security", International Journal of Computer Engineering & Technology (IJCET), pp. 8–19, Volume 9, Issue 1*, Jan-Feb 2018.

[6] Shikha Sharma & Shivani Sharma*,"A Review: Analysis of Various Attacks in VANET", International Journal of Advanced Research in Computer Science, pg 249-253, Volume 7, No. 3*, May-June 2016.

[7] Q Alriyami, A Adnane & A K Smith, *" Evaluation Criterias for Trust Management in Vehicular Ad-hoc Networks (VANET) ",ICCVE 2014*, Nov. 2014

[8] J Grover, M S Gaur & V Laxmi, *" Trust Establishment Techniques in VANET", Wireless Networks and Security, SCT, pp. 273–301*, 2013.

[9] S Gillan, F Shahzad, A Qayyum & R Mehmood, *" A Survey on Security in Vehicular Ad Hoc Networks", Nets4Cars/Nets4Trains 2013, LNCS 7865, pp. 59–74*, 2013.

[10] S. S. Tangade & S. S. Manvi*, "A Survey on Attacks, Security and Trust Management Solutions in VANETs", 4th ICCCNT*, July, 2013.

[11] J Zhang*," A Survey on Trust Management for VANETs", 2011 International Conference on Advanced Information Networking and Applications, pg 105-112*, 2011.

[12] J Jain, N Chahal*,"A review on VANET, types, characteristics and various approaches", International Journal of Engineering Sciences & Research Technology, pg 239-245*, September 2016.

[13] M N Rajkumar, M Nithya, P HemaLatha*, "Overview of VANETs with its security features and attacks", International Research Journal of Engineering and Technology (IRJET), pg 137-142, Volume: 03 Issue: 01*, Jan-2016

[14] M Saini, H Singh*, "VANET, its Characteristics, Attacks and Routing Techniques: A Survey", International Journal of Science and Research (IJSR), pg 1595-1599, Volume 5 Issue 5*, May 2016.

[15] S. Sill, *DSRC: The Future of Safer Driving, Available:https://www.its.dot.gov/factsheets/dsrc factsheet.htm* [Accessed:10-March-2018]

[16] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, *''Trust and exclusion in vehicular ad hoc networks: An economic incentive model based approach,'' in Proc. Comput., Commun. IT Appl. Conf.(ComComAp),pp.13–18*, Apr.2013.

[17] N. Yang*, ''A similarity based trust and reputation management framework for VANETs,'' Int. J. Future Generat. Commun. Netw., vol. 6, no. 2, pp. 25–34*, 2013.

[18] J. Zhang, C. Chen, and R. Cohen*, ''Trust modeling for message relay control and local action decision making in VANETs,'' Secur. Commun. Netw., vol. 6, no. 1, pp. 1–14*, Jan. 2013.

[19] F. G. Mármol and G. M. Pérez, *''TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks,'' J. Netw. Comput. Appl., vol. 35, no. 3, pp. 934–941*, 2012.

[20] S. Gurung, D. Lin, A. C. Squicciarini, and E. Bertino, *''Information-oriented trustworthiness evaluation in vehicular ad-hoc networks,'' in Proc. NSS, pp. 94–108*, 2013.

[21] R. A. Shaikh and A. S. Alzahrani, *''Intrusion-aware trust model for vehicular ad hoc networks,'' Secur. Commun. Netw., vol. 7, no. 11, pp. 1652–1669*, Nov. 2014.

[22] P. Golle, D. Greene, and J. Staddon, *''Detecting and correcting malicious data in VANETs,'' in Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw., pp. 29–37*, Oct. 2004.

[23] U. Khan, S. Agrawal, and S. Silakari, *''Detection of malicious nodes (DMN) in vehicular ad-hoc networks,'' Procedia Comput. Sci., vol. 46, pp. 965–972*, Apr. 2015

[24] H. Sedjelmaci and S. M. Senouci, *''An accurate and efficient collaborative intrusion detection framework to secure vehicular networks,'' Comput. Elect. Eng., vol. 43, pp. 33–47*, Apr. 2015.

[25] A. Jesudoss, S. V. K. Raja, and A. Sulaiman, *''Stimulating truth-telling and cooperation among nodes in VANETs through payment and punish-ment scheme,'' Ad Hoc Netw., vol. 24, pp. 250–263*, Jan. 2015.

[26] N. Kumar and N. Chilamkurti, *''Collaborative trust aware intelligent intrusion detection in VANETs,'' Comput. Elect. Eng., vol. 40, no. 6, pp. 1981–1996*, 2014.