Evaluating Trust-Based Security Measures for VANET Routing

P.Sowjanya[1], Dr.D.M.M.Vianny[2], T.Ramya Priya[3]

[1] Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[2] Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

[3] Assistant Professor, Department of CSE, Sri Indu Institute of Engineering & Technology, Hyderabad

Abstract: ***As Vehicular Adhoc Networks (Vanets) is an ephemeral network in which establishing trust between vehicles is a tedious process. Incorporating mutual trust between nodes is required for secure routing. But malicious nodes in the network cause disturbances during data transmission. Several approaches are existing on trust establishment for secure routing in Vanet. In this survey paper, we have suggested a comparative analysis on existing trust models based on properties. This will help the researchers to have a clear look on this area of research.***

Keywords: Trust, Reputation, Attack, Malicious, Bogus, Efficiency

1. Introduction

One of the most promising and commercialized research area in computer networking is Vanet. This is the subset of Manet under networking. As the population increases the demand over vehicles also increased and has become a necessary thing in our daily life. The increase of vehicle also lead to the increase of minor and major accidents even causes death. So in order to avoid these it is necessary to work on new hardware and software such as equipments, devices, techniques, mechanism, applications, rules and regulations, constraints etc. Basically the message transfer takes place in three ways namely Vehicle to Road Side Unit (V2R), Vehicles to Vehicles (V2V), RSU to RSU (R2R). Based on the content of the message it is subdivided into three types such as added value message which provide numerous services so treated as *Low level*, advertisement message for commercial purpose so treated as *Medium level* and emergency or warning message which carry life safety information to prevent from risky situations so treated as H*igh level*. Depending upon the situation some vehicles may discard the message or accept it but not transmitted or accept it and transmitted to other vehicles. It is not mean that every time the received message is a trusted one. Some messages may be a false, outdated, altered, fun, repeated etc. These messages may confuse the vehicle drivers to take quick decision like whether to continue in the same path or take an alternate path. In addition to that it may consume more space, time, bandwidth etc.

Generally there are two types of attack in Vanet, one is *External* and another is *Internal*. The actions like misuse, manipulation, repair, disconnect, damage etc are termed as External attack. Various types of Internal attacks are available such as message forging, impersonation, packet dropping, black hole, gray hole, worm hole, on - board tampering, in - transit traffic tampering, illusion alteration, bogus, Dos, selfish node, message suppression etc. Trust model is classified into two types, first is *Infrastructure based trust* and another is *Self organizing trust*. Infrastructure is again subdivided into *Centralized* and *Distributed*. Both would work on online and offline. Whereas Self organizing trust is categorized into *Direct*, *Indirect* and *Hybrid*. The Direct method or First - hand information would collect all the needed information by the vehicle itself to determine trustworthy. The Indirect method (or) Second - hand information would gather all the needed information through the opinion given by other vehicles. The Hybrid is the combination of both Direct and Indirect method. So it is necessary for each vehicle to determine whether the received message is the trusted information and from the trustworthy sender. There are many existing protocols are available on trust management which differ in their own way. Some approaches uses PKI include certificates for authentication and authorization, consider reputation to handle all types of events, include cluster algorithm to allot the responsibility, assign probability for uncertainty, use fuzzy logic for accurate results etc. Most of the protocols make use of Reputation and Trust Score to prove their trustworthy. For the score calculation, the following information are gathered such as previous experience from the same vehicle or from other vehicles which follow the same route, getting recommendation or opinion from other neighbor vehicles, collecting recommendation from the Central Authority regarding traffic signals, updated traffic rules and regulations, road condition, agitation etc.

2. Existing Approaches for Trust Management in Vanet

Dijiang Huang [3] et al proposed situation - aware trust architecture for Vanet. The three main components of SAT architecture are Cryptographic Access, Proactive Trust and Social Network. First is to identify common properties from group of vehicles. The second is to distribute certificate before actual communication. The third is to integrate with identity based cryptography. In detail, SAT system construct policy tree which has two parts namely Static and Dynamic part. In proactive SAT system, the Way - point Information framework (WIF) is used to address light time constraints to establish local and global trust. The social network trust provides three functions, one to trust between email user and content, second is to protect user's privacy and third is to interfere SAT into Vanet. Finally the overall performance gain and improve scalability.

Jorge [4] et al recommended in evaluating the usefulness of watchdog for intrusion detection in Vanets. Watchdog is a component used for the detection of selfish nodes and

malicious attackers. This is achieved by supervising the activity of neighbours node's whether they follow routing rule. The design approach of watchdog implies the detection of trusted and untrusted neighbours. Next is minimizing the false watchdog detections by including the devaluation technique to decrease all the oldest received packets. The malicious node is identified when degree of packet loss is greater than the value of tolerance threshold.

Zhou, wang [5] et al developed counter measure uncooperative behaviours with Dynamic Trust Token (DTT) in Vanet. In which the DTT is cooperation enhancement mechanism which detect and prevent misbehaving nodes and protect the integrity of the packets during delivery. There are three roles in DTT namely Predecessor for one - hop upstream node, Relayer for packet forwarding and Successor for one - hop downstream node. DTT uses neighbourhood watchdog for generating trust token and both symmetric and asymmetric encryption for integrity. In summary, this is a passive detect - & - react mechanism which prevents packet containing false information. Once the malicious node is identified it lacks in neither punishing it nor reward the well - behaved node.

Subir, Biswas [6] et al designed an ID - based safety message authentication for security and trust in Vanet. This is one of the approach having certificate less public key verification for message authentication and trust management. Elliptic Curve Digital Signature Algorithm (ECDSA) is based on Elliptic curve crypto system. It is an ID - based system which is no need to store, fetch and verify Public Key Infrastructure (PKI) certificate. In this algorithm the following assumption is made ie RSU are independent of each other, verification of message using location information and forward signature materials to other Vanet entity. In short, this algorithm saves storage space, communication bandwidth and reduces time complexity.

Yu - Chih [7] et al suggested an efficient trust management system for balancing the safety and location privacy in Vanet. This approach is called RaBTM ie Rsu and Beacon based Trust Management system which detect the trustworthy vehicles by the opinion gathered from other vehicles. This system maintains the accuracy and reduces the delay in finding the trustworthiness. This is highly resilient from bogus and alternation attack which decreases the transportation efficiency and causes accidental events. Trust information gathering methods are categorized into three types namely Direct method or First - hand information which gather trusted information by vehicle itself. Next is Indirect method or Second - hand information which gather opinion from others. Finally Hybrid method, is a combination of both Direct and Indirect method. In summary, this approach is highly resilient to various attacks, make decision quickly and give opinion with short delay.

Felix, Gomez [8] et al designed a Trust and Reputation Infrastructure based Proposal [TRIP] for Vanet. This will identify malicious and selfish nodes which broadcast bogus information to other nodes. The central authority will take care of malicious database with frequent updates. There are three types of assessment made on received message. First, to reject or drop the message, second to accept but not forward and third to accept and forward. Based on the assessment the trust level is categorized into three levels namely Not trust, Trust and +/ - Trust. This is followed by the calculation of reputation and trust score. The evaluation of reputation score is by taking previous experience or recommendations from other vehicles or recommendations from central authority. Even the content of the message specify three severity levels namely High level which hold accident warning content. Next Medium level holds the advertisement regarding messages and finally Low level holds less important message where both are treated as +/ - Trust level. In short, TRIP is a simple, light, fast and scalable trust and reputation mechanism.

Dhurandher [9] et al recommended a reputation and plausibility checks - based approach on securing Vanet. Vehicular Security through Reputation and Plausibility checks [VSRP] handle data aggregation and data dropping. In VSRP approach, three different checks are performed namely Timestamp to identify whether it is an old or new message, Transmission delay whether within the active area or not and Velocity of the nodes to judge their movement. Another algorithm is included in this approach named as Vehicle Adhoc network Reputation System [VARS]. VARS defines three areas namely Event areas where an event is recognized, Decision area where the trustworthiness of event message is judged and Distribution area denotes how far an event message is distributed. A message with plausibility problem is identified and solved by plausibility validation model where many rules are specified. The message events are categorized into three types namely Single - hop which hold application of brakes, Multi - hop represents traffic jam and accidents, and Malicious contains misbehavior. In short, VSRP improves confidence in decision making, eliminate false attack, handle packet drop with reduced overhead.

Gazdar [10] et al suggested secure clustering scheme based keys management in Vanet. The Vanet Dynamic Demilitarized Zone (VDDZ) algorithm filters the certificate request directed to CA and protects direct communication and different types of attacks. This is a PKI based trust model and clustering algorithm. Each cluster contains four roles namely Certification authority act as cluster head, Registration authority which protects CA from attackers, Gateway obtain communication between two adjacent clusters and Member node within a cluster. The VDDZ approach is robustness in architecture and detects and prevents Dos or jamming attack.

Qing, Ding [11] et al developed reputation based trust model in Vanet. This algorithm is an event - based reputation model which filters bogus warning messages. This approach categorizes the entire event to different roles. A reputation is specified for each role. Such roles in cluster are Event Reporter (ER) which estimate the importance of traffic event and set the reputation value. Event Observer (EO) which identify bogus event messages and Event Participant (EP) which is beyond one - hop so it cannot predict the behavior of ER. In summary, this approach filters bogus message and propagate accurate and reliable traffic warning messages.

Jian, Wang [12] et al suggested a trust propagation scheme in Vanet. Each user possess the following attributes such as

location, energy and brand. Based on the attribute values a trust scale is generated between 0 and 1. The stronger trust event will receive the highest trust degree. The main objective of this algorithm is to evaluate the attributes, check and calculate the similarity between nodes. In short, this algorithm determines the routing path, computing similarity degree of attributes, forwarding packets and recognizing forwarding behaviours.

Serna [13] et al designed geolocation - based trust for Vanets privacy. The Vehicular Information Transport Protocol (VITP) has two mechanism. One is mandatory access control model and another is novel geolocation - based information from certification and attributes authority. Under first one, the authorization is divided into three levels, namely Personal level carry private information, Emergency level carry safety information and Public carry general information. In second, the trust anchor will validate and trust certificate for authentication and authorization using PKI. The two main task of interoperability system is online validation of the certificate and issuing security level.

Gazdar [14] et al suggested a trust - based architecture for managing certificates in Vanet. This is a secure and distributed PKI based on hybrid trust model to find Trust Metric (T_m). T_m is based on two aspects such as Cooperation of vehicles by calculating the forwarding rate another is Accuracy of broadcasted data by using fuzzy set theory. A fuzzy - based solution will accurately portray the vehicle honesty. When any node having only one neighbour is recommended as certificate authority. PKI with third party CA provide high level of trust worthies. There are three types of membership namely Registration authority to protect from unknown and malicious vehicle, Gateway through which all the packets are passed and Member node are ordinary simple members in a cluster. This approach achieves the efficient and stability of clustering algorithm.

Yi - Ming, Chen [15] et al developed a beacon - based trust management system for enhancing user centric location privacy in Vanet. This approach establishes message transmission send with cryptography and the pseudo identity scheme. This is mainly concentrated on three types of attacks namely Alteration, Bogus and Message suppression. Secure Beacon Authentication Protocol (SBAP) uses pseudo identifiers and changed regularly. This protocol uses Medium Access Control (MAC) and ECDSA. Even though this protocol provides vehicle privacy but complicate in storing anonymous keys and increase the cost of key management. Trust relation is divided into two types, one is Direct event and other is Indirect event based trust. Trust worthiness is obtained by combining data - centric trust establishment scheme and Dempster - Shafeer Evidence (DSE). This is more suitable for fixed and random silent privacy.

Chen [16] et al proposed secure and efficient trust opinion aggregation for Vanet. This approach is based on the existing identity - based to aggregate signature algorithm which combines multiple signatures into single signature and send to the vehicles. Aggregation of trust opinion helps to detect data repudiation, any provider cannot deny its message and identities cannot be forged before sending any packets. Efficiency of trust opinion is based on two aspects, one is Time efficiency ie performing aggregation without any delay and second is Space efficiency ie aggregate all trust opinion and signature by removing old and unwanted messages. But the use of aggregation achieves high security with space overhead. This approach needs only a list of identities and the final aggregate signature remains unique and accurate. So whenever a new emergency message is signed vehicles will generate pseudonym to hide their identities. In summary, this approach achieves high security, flexible aggregation, and time and space efficiency with minimum additional information by eliminating redundancy.

Rashmi, Sahoo [17] et al proposed a trust based clustering with ant colony routing in Vanet. The trust dependent ant colony routing algorithm selects the most appropriate Cluster Head (CH) using real time updated position, trust value, speed and radio range. The selected CH operates on two different frequencies in avoiding intra and inter message communication. But the selection of CH needs re - affiliation energy, velocity, trust value of vehicle and efficient message communication. The size of a cluster is based on the speed of the vehicle which plays an important role in network stability. This approach uses dynamic transmission range which takes advantage of power savings by increasing their capacity. Generally it is determined on the vehicle movement and speed. It uses a bio - inspired ant colony routing procedure to detect malicious vehicles and makes use of indirect trust for trust value calculation. Finally to say this is one of the algorithm which deals with scalability issue.

Table 1 shows a comparative analysis of existing trust models against the desired properties for secure routing in Vanet.

3. Desired Properties for Effective Trust Management in Vanet

- Decentralized – The environment is highly dynamic and distributed which is controlled by several local stations to take over the control.
- Sparsity – There may be some shortages in the environment.
- Dynamics – Taking a sudden action based on the current situation.
- Scalability – Establishing a wide connection for communication and transmission.
- Confidence – Believing all the nearest neighbours as the trusted one.
- Security – The state of feeling safe and free from various attacks.
- Privacy – Safeguarding all the details of vehicle owner's identity.
- Robustness – Being strong and good condition which protect them from different attacks.
- Reputation – Way of rating each other to build trust
- Efficiency – shows reasonable time and allowable space
- Stability – remain in same state without any disturbances

Table 1: A survey of trust establishment approaches

Approaches	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]
Decentralized	√							√				√		√	
Sparsity		√				√						√	√		
Dynamics	√		√			√		√			√		√	√	√
Scalability	√	√	√	√	√	√	√		√	√		√	√	√	√
Confidence	√	√	√	√	√	√	√	√	√	√	√	√	√	√	
Security	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√
Privacy	√		√	√	√	√		√	√		√		√	√	√
Robustness	√	√	√	√	√	√	√	√	√		√	√	√		√
Reputation						√	√		√				√		
Efficiency		√	√	√	√		√	√			√	√		√	
Stability						√		√				√			

4. Conclusion

In Vanet, establishing a trust management is most pivotal for secure routing. Malicious nodes may broadcast bogus messages throughout the network which may lead from trivial to significant problems. We have proposed a list of some important properties and made comparison with the existing trust models. From the analysis we have come to a conclusion that a narrow - down research work is needed on the stability of trust models. Our research will help to develop an effective trust management in order to enhance the road safety.

References

[1] Nirav J. Patel, Ratvij H. Jhaven, “Trust based approaches for secure routing in vanet: A survey”, International conference on advanced computiting technologies and applications (ICACTA), pp - 592 - 601, 2015.

[2] Jie Zhang, “A survey on trust management for vanets”, International conference on advanced information networking and applications, pp - 105 - 112, IEEE 2011.

[3] Hong, Xiaoyan, Dijiang Huang, Mario Gerla, and Zhen Cao, "SAT: situation aware trust architecture for vehicular networks ", In Proceedings of the 3rd international workshop on Mobility in the evolving internet architecture, pp - 31 - 36, ACM, 2008.

[4] 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, IEEE, 2010.

[5] Wang, Zhou, and Chunxiao Chigan, "Countermeasure uncooperative behaviors with dynamic trust - token in VANETs", In Communications, ICC'07, IEEE International Conference on, pp - 3959 - 3964, IEEE, 2007.

[6] 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 International Conference on, pp - 323 - 331. IEEE, 2011.

[7] Wei, Yu - Chih, and Yi - Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", In Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference on, pp - 393 - 400. IEEE, 2012.

[8] Gómez Mármol, Félix, and Gregorio Martínez Pérez, TRIP, a trust and reputation infrastructure - based proposal for vehicular ad hoc networks ", Journal of Network and Computer Applications 35 springer, no.3 pp - 934 - 941, 2012.

[9] Dhurandher, Sanjay K., Mohammad S. Obaidat, Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi, "Securing vehicular networks: a reputation and plausibility checks based approach", In GLOBECOM Workshops (GC Wkshps), IEEE, pp - 1550 - 1554, IEEE, 2010.

[10] Gazdar, Tahani, Abderrahim Benslimane, and Abdelfettah Belghith, "Secure clustering scheme based keys management in VANETs", In Vehicular Technology Conference (VTC Spring), IEEE 73rd, pp - 1 - 5. IEEE, 2011.

[11] Ding, Qing, Xi Li, Ming Jiang, and XueHai Zhou, "Reputation based trust model in vehicular ad hoc networks", In Wireless Communications and Signal Processing (WCSP), International Conference on, pp - 1 - 6, IEEE, 2010.

[12] Wang, Jian, Yanheng Liu, Xiaomin Liu, and Jing Zhang, "A trust propagation scheme in VANET s ", In Intelligent Vehicles Symposium, IEEE, pp - 1067 - 1071, 2009.

[13] Serna, Jetzabel, Jesus Luna, and Manel Medina, "Geolocation - Based Trust for Vanet's Privacy", In Information Assurance and Security, ISIAS'08, Fourth International Conference on, pp - 287 - 290. IEEE, 2008.

[14] Gazdar, Tahani, Abderrahim Benslimane, Abderrezak Rachedi, and Abdelfettah Belghith, "A trust - based architecture for managing certificates in vehicular ad hoc networks", In Communications and Information Technology (ICCIT), International Conference on, pp - 180 - 185., IEEE, 2012.

[15] Chen, Yi - Ming, and Yu - Chih Wei, "A beacon based trust management system for enhancing user centric location privacy in VANETs", Communications and Networks, Journal of 15, no - 2 pp - 153 - 163, 2013.

[16] Chen, Chen, Jie Zhang, Robin Cohen, and Pin - Han Ho, "Secure and efficient trust opinion aggregation for vehicular ad - hoc networks", In Vehicular Technology Conference Fall (VTC 2010 - Fall), 2010 IEEE 72nd, pp.1 - 5. IEEE, 2010.

[17] Sahoo, Rashmi Ranjan, Rameswar Panda, Dhiren Kumar Behera, and Mrinal Kanti Naskar, "A trust based clustering with Ant Colony Routing in VANET", In Computing Communication & Networking Technologies (ICCCNT) Third International Conference on, pp - 1 - 8 IEEE, 2012.