A Survey on Trust Based Data Forwarding in VANET

[1]Poonam Dabas
[1]Assistant Professor, CSE Department, UIET, Kurukshetra University, 136119, Kurukshetra, Haryana
Email:poonamdabas.kuk@gmail.com
[2]Aman Kumar
[2]M.Tech Student, CSE Department, UIET, Kurukshetra University, 136119, Kurukshetra, Haryana
Email:aman.sagwal92@gmail.com

Abstract

VANET is vehicular ad hoc network in which vehicles are move from one place to another place and carry messages that are transmitted from one vehicle to another vehicle. To transfer messages to vehicles uses ITS (Intelligent Transportation Systems). During data transmission data or information may be accessed by attackers. So Security in VANET is challenging task. Various techniques are proposed by researchers to prevent VANET from attacks. Every system has its own component and also upsides and downsides. These techniques are discussed in detail after that we discussed our proposed mechanism for trust based data forwarding.

Keywords: VANET (Vehicular Ad hoc Network), ITS (Intelligent Transportation Systems), Certification Authorities (CA) and Reputation.

1. Introduction

Vehicle interchanges are turning out to be progressively well known pushed by route security necessities and by the speculations of producer and open transport powers [1]. Vehicular Ad-hoc Networks (VANET) has significant potential to enable diverse applications to ameliorate the driving experience. Compared to the traditional wireless networks, VANET can provide enhanced flexibility and capacity in information delivery between vehicles or among vehicles and infrastructure. In vehicular networks, WAVE Standards [2] form the basis for the implementation of a wide set of applications in the transportation domain, they include vehicles security, regular tolls, enhanced steering, transfer organization and several applications [3].However, vehicular networks are facing up a lot of challenges. As many vehicular applications are directly connected to driving security, it is of high value to implement security mechanisms properly. due to its plasticity and infrastructure-independent nature, VANETs are particularly vulnerable to various attacks compared to conventional networks. In recent years, the discussion about vehicular security is mainly about privacy protection and the encryption of sensitive information. As a result, the Public Key Infrastructure (PKI) which provides certificate management by using the Certificate Authority entities (CA entities) [4] variants of encryption algorithms and privacy preserving schemes are proposed which can improve the trustworthiness of vehicular networks. However, as a wireless access networking, the bottle neck of vehicular networking is the availability of the resources. The possible attack such as passive eavesdropping, denial of service (DoS) and the black hole attacks can all increase the packet drop rate and cause catastrophic damage to the vehicular infrastructure. Moreover, these type of attack are always easy to launch and not easy to defend.

1.1 Network Security

Network security is the computer security as well as secures correspondence between the PCs or different gadgets. Not all hubs are PCs in an Ad Hoc system, in these way nodes can't be accepted to execute the security administrations normally existent in computers' operating systems. That is why network protection have to be defined as: Making sure that the nodes enforce a proper computer security and then securing the communication between them.

To offer a safe networking atmosphere following services are required:

i. Authentication: A node must identify with whom it is communicating with.
ii. Confidentiality: Information is never revealed to intruder i.e. third party, only sender and receiver are communicating.
iii. Integrity: The sent message have not to be changed in between the transmission.
iv. Non-repudiation: After transfer the information, the sender cannot refuse and after receiving the information, the receiver cannot refuse.
v. Availability: All Nodes have to be accessible all the ideal opportunity for correspondence. A hub need keep on providing administrations regardless of assaults e.g.: key administration.
vi. Detection and isolation: Protocol must determine nasty nodes and separate them, so that they cannot get in the way with routing.

1.2 Classification of various attacks: In this part we present various types of attacks on the base of their behavior. These are as follows [5]:

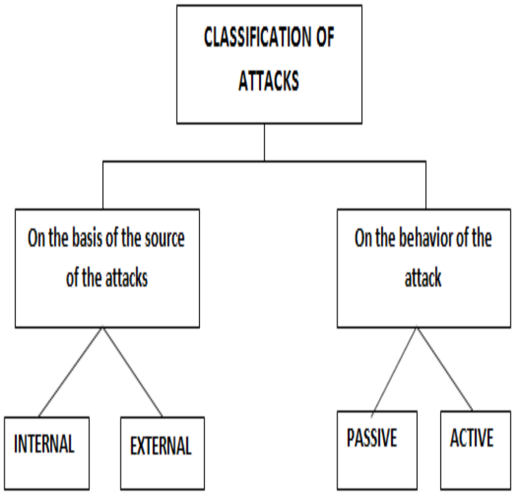
CLASSIFICATION OF ATTACKS
On the basis of the source of the attacks
On the behavior of the attack
INTERNAL
EXTERNAL
PASSIVE
ACTIVE

Fig 1: Classification of Attacks

External and Internal Attack: In external attack attacker wants to access network information by keeping themselves from outside network. Internal attack is caused by nodes which behave maliciously in between network. The main aim of them, are just to contribute in the regular actions of the network.

Active and Passive Attack: In active attack attackers perform attack to access network information and change network information. In passive attack attackers just monitor data transmission occurred in network. In this attack they do not disturb data transmission [6].

1.3 Other kind of attacks:

i. Black hole attack: In this type of attack wrong routing information is sent by attackers during data transmission in network.
ii. Sybil Attack: A Sybil attack is a attack in which attacker forge identification of normal node and behave as that normal node.
iii. Selfish node attack: In this type of attack selfish node cannot forward messages to other node to in order to save its energy.
iv. Worm hole attack: In worm hole attack duplicate copies of message is generated by attacker to access the actual information of user.

2. Related work

G. Guette et al. [7] planned TPM based security structural design to solve the issues of security and privacy for successful deployment of VANET technology. Its objective was to focus on management of cryptographic keys and to provide security and anonymity in vehicles communication.

Tamilselvan et al. [8] proposed PCBHA (Prevention of a Co-operative Black Hole Attack) based on the AODV protocol to prevent cooperative black hole attacks. Moreover, some intrusion detection or reputation score based solutions are proposed.

Liu et al. [9] proposed a street side foundation construct structure chiefly centering with respect to framework administration, creators utilize independence premise to convey, order and oversee in a locale extending from a city region to the entire nation. The structure is exceptionally adaptable, convention free and backings basic affirmation, for example, bunch signature, character based confirmation, pen name, and so on proposed plan was worked just in constrained base present yet fizzled in when long framework present.

Chen et al. [10] have also proposed a similar approach but they employed a cluster-based routing protocol for message propagation. A cluster head can only decide whether or not to relay the message based on the calculation of trust. Trust calculation is also based on the aggregated opinions appended to the message as well as the cluster head's local opinion. The problem with Chen's approach is that they did not show the way in which entities can accurately estimate the confidence value of the opinion aggregated by previous entities, despite the importance of the confidence value in helping to model uncertainty of the opinions.

3. Trust management schemes

In VANET various trust management techniques are presented to prevent network from malicious activities caused by various attackers. These techniques are:

i. Reputation based trust management scheme: In reputation based mechanism each node give opinion of its neighbor node by checking their reputation value and classify whether it is malicious node or normal node. The drawback of this scheme is that measuring reputation of node is difficult task because of active environment of vehicles [11].

ii. CORE: In this technique node forward the packet by keeping track of other nodes and their movement. Drawback of scheme is that sender node depends on another node and if another node is malicious then transmission may cause [12].

iii. Buddy System: this technique is based on social structure means how one node depends on another node. Based on this it is to be decided whether node forwards the packets or not. Drawback of this scheme was that measuring contact between two nodes/vehicles because of active environment of vehicles [13].

4. Proposed work

Different researchers proposed various techniques for detection and prevention of VANET from various kinds of attacks. Some of them designed methodologies for the calculating the trust between nodes during routing. Each one has its own advantages as well as drawbacks based on their work we will try to propose a enhance algorithm for calculating trust in VANET. In our proposed work we present a trust model based on the perception of trust degree and apply this model to opportunistic routing in VANET. Our model builds a trust relationship for each node with all its neighbors and recommended trust degree. The proposal improves the trust evaluation process for nodes. VANET are ephemeral networks: this means that the connections between nodes (vehicles) are short-lived. Limitations occurred during data transmission in VANET:

In most cases, node A will never meet node B again.

The network topology is constantly changing as nodes move in and out of communication range.

The node density changes throughout the day: higher in the peak hours during the day and lower at night.

Vehicles can have more expensive/powerful processing devices than regular nodes in ad hoc networks. Therefore, more complex calculations can be easily implemented.

Since the drivers and owners of the vehicles are human beings, it can be assumed that the human behavioral tendencies will be reflected in the behavior of each node.

Each node has its own buffer (temporary memory) to store messages during data transmission. Node stores information like no of messages received, no of messages created, no of messages delivered, no of messages acknowledged. By checking node history from their buffer we compute their some value. On the basis of these values we decide the next node through which data is transmitted. For this I propose a new algorithm and compare it with existing scheme.

TABLE1 nodes with reputation value

Nodes	Reputation value
Node 1	0.21
Node 2	0.41
Node 3	0.14
Node 4	0.47
Node 5	0.36
Node 6	0.98

Above table show that reputation value of each node computed on the basis of above mentioned information. Next compare node reputation value with some unique hint value and calculate trusted node and untrusted node.

5. Conclusion

Security of vehicles in VANET is a testing undertaking. In this paper different sorts of assaults are talked about after that diverse trust administration plans with their favorable circumstances and inconveniences has been introduced. Near investigation demonstrate that notoriety based system is more secure than different methods. Next we show our proposed work to compute trust between nodes in light of notoriety component.

References

[1] M. Raya, Data-Centric Trust in Ephemeral Networks. Ph D Thesis. EPFL, Lausanne, 2009.

[2] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, “Aema: An aggregated emergency message authentication scheme for enhancing the security of vehicular ad hoc networks,” in ICC, 2008, pp. 1436–1440.

[3] A. Wasef and X. Shen, “Maac: Message authentication acceleration protocol for vehicular ad hoc networks,” in GLOBECOM, 2009, pp. 1–6.

[4] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, “Architecture for Secure and Private Vehicular Communications,” in IEEE International Conference on ITS Telecommunications (ITST), Sophia Antipolis, France, June 2007, pp. 1–6.

[5] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure Vehicular Communication Systems: Design and Architecture,” IEEE Communcations Magazine, vol. 46, no. 11, pp. 100–109, November 2008.

[6] L. Butty´an, T. Holczer, and I. Vajda, “On the effectiveness of changing pseudonyms to provide location privacy in vanets,” in ESAS,

ser. Lecture Notes in Computer Science, vol. 4572. Springer, 2007, pp. 129–141.

[7] G. Guette and C. Bryce, “Using TPMS to Secure Vehicular Ad Hoc Networks (VANETS)”, in: Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks, 2008, pp: 106-116.

[8] L. Tamilselvan and D. V. Sankaranarayanan, “Prevention of Cooperative Black Hole Attack in MANET,” Journal of Networks, vol. 3, no. 5, Jan 2008, pp: 13–20.

[9] Wenmao Liu, Hongli Zhang and Weizhe Zhang, “An Autonomous Road Side Infrastructure Based System in Secure VANETs”, 978-1-4244-3693-4/09/$25.00,2009 IEEE, pp: 1-6.

[10] Chen et al, “A Trust Modeling Framework for Message Propagation and Evaluation in VANETs”, Proceedings of the International Conference on Information Technology Convergence and Services, 2010, pp: 1-8.

[11] N.-W. Lo and H.-C. Tsai, “A reputation system for traffic safety event on vehicular ad hoc networks,” EURASIP - Journal on Wireless Communications and Networking, 2009.

[12] M. Raya, R. Shokri, and J.-P. Hubaux, “On the tradeoff between trust and privacy in wireless ad hoc networks,” in WISEC. ACM, 2010, pp. 75–80.

[13] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in MOBICOM, 2000, pp. 255–265.

[14] P. Michiardi and R. Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in CMS, 2002.

[15] S. Fahnrich and P. Obreiter, “The buddy system - a distributed reputation system based on social structure,” Universitat Karlsruhe, Faculty of Informatics, Tech. Re`p., February 2004.