IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

A Review on Trust Management in VANET

Deepa Soni[1], Ravindra Gupta[2], Varsha Namdeo[3]

Research Scholar, Dept. of CSE RKDF IST Bhopal (M.P)[1]

Assistant Professor, Dept. of CSE RKDF IST Bhopal (M.P)[2]

HOD, Dept. of CSE, RKDF IST Bhopal (M.P)[3]

Abstract: There is an pressing need of effective trust management for vehicular ad-hoc networks (VANETs), given the dire consequences of functioning on false data sent out by malicious peers during this context. In this paper, we have a tendency to initial discuss the protection & study of assorted attacks in VANET and comparison of assorted attacks in VANET. We tend to then survey of VANET Security needs & trustworthy computing to boost security in network. Supported these studies, we recommend desired properties towards effective trust management in VANETs, putting in clear goals for researchers during this space.

Keywords: V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), RSU (road side unit).

I. INTRODUCTION

Traffic congestions, road accidents and maintenance, are the most important issues of current traffic systems, within which drivers ought to be totally responsive to the encompassing surroundings. Vehicular ad hoc networks (VANET) square measure a category of ad- hoc networks. In VANETs, there are two varieties of communication [1]: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) additionally referred to as vehicle to roadside unit (V2R), as shown in Figure 1. In V2V communication vehicles send and receive messages to and from each other. These messages may be coverage road congestion, accidents ahead, etc., referred to as safety messages. V2I communications are between nodes and road aspect infrastructure, e.g. coverage an incident or a malicious node, finding nearest petrol station, on-line toll payment, etc. transport communications consists of vehicles (nodes), road aspect units (RSUs). An RSU is employed for broadcasting emergency road-safety messages, modified road-condition notifications, neighborhood info, etc

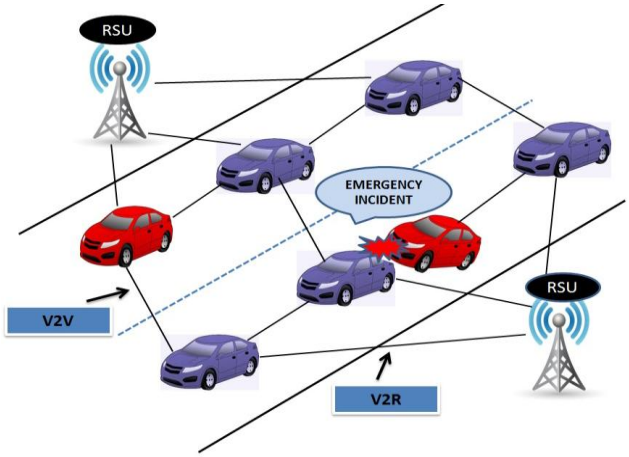

Figure 1 VANET Model

It is necessary for vehicular ad hoc environments to make sure traffic safety, by delivering the proper info to drivers in a very measurable effective time. This is often not continually simple because of the presence of malicious or greedy nodes, wherever false info may be broadcasted dishonest nodes within the scene. Thus, establishing trust between nodes is an important considers order to work out whether or not their claimed sent info is reliable [2].

II. SECURITY IN VANETS

Message authentication [3] and information integrity [4] are necessary security needs in VANET applications. Message authentication guarantees that the message comes from its original sender, signed by his own non-public keys. Message

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

integrity means that the content of the message shouldn't be altered throughout its transmission from the sender to receiver. Safety messages and proper event coverage play a very important role in vehicular systems. Applying smart authentication technique and guaranteeing message integrity couldn't stop deceptive message content from being broadcasted.

III. SECURITY ATTACKS IN VANETS

Vehicular ad hoc Network (VANET) serves user with safety and non safety applications however wants security to implement the wireless surroundings In VANET vehicles doesn't have fixed infrastructure as a result of the explanations that vehicles are nodes with quality. It serves safe and non safe wireless applications as a result of that security is most significant concern in VANET. During this paper we are going to present comprehensive study of assorted attacks in VANET and comparison of assorted attacks in VANET. [4]

A. Denial of Service (DOS): It is the most serious level attack in vehicular network. This kind of attack is extremely| easy however it's very harmful. It will stop necessary info from incoming. During this attack its use different identity and block the services of different or it will stop additionally VANET communication service. These attacks done by attackers taking management of others and stop the communication services or jam the channel in network. This attack is extremely harmful to the drivers that aren't act and additionally get false data. [5]

B. Distributed Denial of Service Attack (DDOS Attack): DDOS attacks are those attacks during which attacker attacks in distributed manner from completely different locations. Attacker might use completely different timeslots for sending the messages. Nature and time interval of the message may be varied from vehicle to vehicle of the attackers. The aim of attacker is same as DOS attack. [5]

C. Sybil Attack: It is an essential attack. During this kind of attack attacker sends multiple messages to different vehicles. Every message contains totally different source identity. It creates confusion to alternative vehicles by causing wrong messages like traffic congestion. so there's jam additional and vehicles are forced to require another route. The main aim of the attacker is to produce an illusion of multiple vehicles to alternative vehicles so vehicles will select another route. [6]

D. Node Impersonation Attack: In vehicular network every vehicle has distinctive identifier that is employed to verify the messages whenever the accident happens by causing the incorrect messages to alternative vehicles. [7]

E. Wormhole Attack: In wireless networking, the wormhole attack consists in tunneling packets between two remote nodes. In VANETs, an attacker that controls a minimum of two entities remote from one another and a high speed communication link between them will tunnel packets broadcasted in one location to a different location. [8]

F. Black Hole Attack: Black hole attack is kind of routing attack and might bring damage to whole network. once some malicious user enters into the network and stop forwarding messages to next nodes by dropping messages are referred to as black node.[8]

G. Grey Hole Attack: Grey hole attack is that the reasonably denial of service attack. During this attack, the router that is mesh behaves simply not well and a set of packets are forward and handle by receiver however leave by others. [9]

H. Application Attack: The main motive of attacker during this reasonably attack is to content that are associated with safety and non safety connected applications. Safety applications play important role as they supply warning messages to different users. During this attack the attackers alter the contents of the particular message and send wrong messages to different users. [8]

I. Timing Attack: The main objective of attacker is makes delay within the original message and these messages are received when these need a time. AS we all know safety applications are time important applications if delay happens in these applications then major objective of those applications is additionally finished. [8]

IV. VANET SECURITY REQUIREMENTS

Confidentiality: In VANET's the term confidentiality refers to the confidential communication. In a cluster nobody except the cluster members are ready to decode the messages that are broadcasted to each member of the cluster. [8]

Integrity: This term refers that data or information among nodes doesn't seem to be altered by attackers. [10]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Availability: It means that network ought to be accessible to the users although it's attacked by the attacker. [8]

Privacy: User privacy is extremely necessary consider vehicular surroundings if once the users' privacy is lost, it's terribly difficult to re-establish. Privacy in VANET is to secure the user's personal information and his/her location. Users would like privacy and should not enable seeing their personal information and their locations. [8][10]

Trust: Last demand is trust and trust [10] is that the key component of security system. once users receive any message from alternative vehicle or from infrastructure it should be trusty as a result of user reacts consistent with the message. to determine the trust, it's needed to produce trust between the users within the communication of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). The attackers modify the contents of the message and break the trust between the Vehicles.

V. TRUST MANAGEMENT

Trust is that the key component in making a trusty vehicular environment that promotes security in vehicular networks. Trust is either in human behavior or within the deployed hardware, wherever each type a trusty communication environment. Trusty computing may be a comparatively new technology that has gained quality recently. The main aim of trusty computing is to boost security in network. [11]

Trusted computing needs two basic properties are fulfilled:

- The sender who sends the data in vehicle to vehicle or vehicle to infrastructure is accepted as a trusty entity.
- The contents of the message supply isn't modified throughout transmission, it meets the integrity demand.

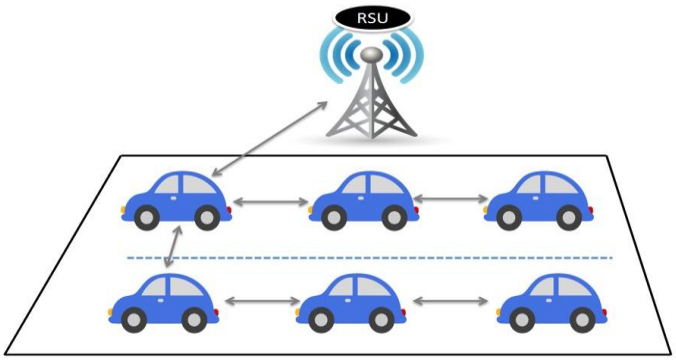

Figure 2 Vehicular Trusted Computing

Trusted Entities of VANET

Basic entities of trust and once of these entities work along then can develops a network of trust within the vehicular network. [12]

Trusted User: Trusted Users (TUs) are those people that perform their task properly within the network. In vehicular environment the user role is very important for building the chain of trust. Chain of trust would be affected if user isn't playing their task accurately. [12]

Trusted Vehicle: The role of vehicle is very important altogether varieties of communication in network. At the fundamental level of trust is to produce security within the vehicle (Trusted Vehicle) and communications are carried through trusted channels between the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I). Trusted Vehicle needs some specific sensors to be a neighborhood of VANET. [13]

Trusted Applications: Safety and non safety applications are serve the users and build their journey safe and comfy. Active safety applications, warning applications and position based mostly routing need security from attackers and user trust are building once these applications perform their task accurately. [13]

Trusted Routing: Routing is essential a part of VANET and message moves from one vehicle to alternative vehicle by using totally different route. Routing involve from hop to hop communication and hop to multi-hop communication, open medium and dynamic configuration makes the routing task is complicated. Secure and trusted routing is critical for sending and receiving safety messages within the network. [8]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 6, June 2017

Trusted Medium: Each vehicle within the network receives messages from different vehicles or from infrastructure. A secure and trusted content of message is that the major concern of the users. The attackers can attempt exhausting to alter the contents of the message and break the trust between the vehicles. once users receive any info (safety or non safety) from different vehicles or from infrastructure it should be trusted as a result of user reacts according to the message. to determine the trust, we have a tendency to should offer secure and trusted channel (Trusted Medium) between the users in network. Whenever attackers launch any variety of attack then we've got the choice of using others channels. [8]

Trusted Infrastructure: Network Infrastructure is very important to verify the users and providing the correct info to users on the road. Infrastructure should be created trusty before they send safety connected info to users, as a result of all users believes it. The target of trusted infrastructure is to confirm the protection of the channel and knowledge being passed among the users. There are many varieties of trust within the vehicular network and therefore the level of trust can increase if we are able to ascertain the management of attackers from launching any attacks. [12] [13].

VI. LITRATURE REVIEW

There is such a variety of trust administration and scrambled confirmation information gathered systems.

Sumra et al. [14], states that if trusty node A communicates with node B safely, then node B becomes trusty. Thus, it provides chain of trust between communication clusters of nodes. The disadvantage of this protocol is that the initial communication node with the new comer node, can always be the victim. Moreover, in vehicular environment nodes are extremely dynamic, continuously leaving a cluster }and connection a brand new cluster. So a malicious node will be part of a replacement cluster that don't have any plan regarding its dangerous history, and deceive nodes at this new cluster..

Sumra et al. [15] depends on a 16 digit code to make sure a secure key renewal. The most disadvantage of this resolution happens at the entry purpose wherever client and service supplier authentication task is performed; the channel might be full once range of users will increase, e.g. in a highway.

Biswas et al. [16], states that if an emergency road-safety application message is generated by a trustworthy central authority, the issued message is broadcasted by RSUs to nodes on behalf of the creator of the message. this can be called partial delegation of authorities. this technique is temporary, as a result of when the broadcasting task ends, it's not clear that nodes are trusty.

Wenjie Wang, Tao Luo, Ying Hu [17] They propose a novel routing protocol in city VANET named Landmark-based routing using global real-time traffic (LRRT), which is beaconless and AP-assisted. Initial of all, we have a tendency to present a density estimation scheme to know the worldwide density info for planning routing protocol. Vehicles in the network periodically update their locations and report back to APs, whereas APs gather these real time reports in their coverage so as to make native density table.
Then the worldwide density info is available by sharing native density info between adjacent APs. Moreover, we have a tendency to style LRRT for knowledge transmission. Once upon knowledge transmission, vehicles apply to APs for the worldwide density info that is used to weight the length of all potential roads from source to destination. The shortest path algorithmic rule Dijkstra is given to output the optimized route that consists of a series of consecutive junctions on the overlay network.

Zubair Amjad "Context Aware Data Aggregation in Vehicular Ad-hoc Networks" [18] Data aggregation for VANETs is taken into account a significant building block for several applications because of its bandwidth saving potential. They propose a unique context aware knowledge aggregation technique for VANETs. the information aggregation is finished by the cluster head based on the context i.e. vehicle speed and density to reduces the desired bandwidth for periodic knowledge dissemination. The projected technique is valid through intensive simulations and results show that context aware knowledge aggregation will considerably reduce communication value.

Jie Zhang [19] "A Survey on Trust Management for VANETs" There is an urgent want of effective trust management for vehicular ad-hoc networks (VANETs), given the dire consequences of working on false data sent out by malicious peers during this context. in this paper, they have a tendency to initial discuss the challenges for trust management caused by the necessary characteristics of VANET environments. They have a tendency to then survey existing trust models in multi-agent systems, mobile ad-hoc networks (MANETs) and VANETs, and denote their key problems. Supported these studies, we recommend desired properties towards effective trust management in VANETs, fixing clear goals for researchers in this area.

Ranjitha. P [20] VANETs have emerged as a promising approach to increasing road safety and efficiency. this could be accomplished in a kind of applications that involve communication between vehicles, like warning alternative vehicles regarding emergency braking etc. Message authentication could be a common tool for making certain data reliableness, namely, knowledge integrity and legitimacy. Once the quantity of messages that area unit received by a vehicle becomes massive, ancient authentication might generate unaffordable process overhead on the vehicle and so bring unacceptable delay to time-critical applications. Associate degree economical cooperative authentication theme for VANETs is adopted. to reduce the authentication overhead on individual vehicles and shorten the authentication delay, the theme maximally eliminates redundant authentication efforts on identical message by totally different vehicles. To resist varied attacks, and encourage cooperation, the theme uses associate degree evidence-token approach to regulate the authentication employment, while not the direct involvement of a trustworthy authority (TA).

VII. CONCLUSION & FUTURE SCOPE

Security of VANET is a very important issue to be addressed by designers of VANET infrastructure security. It will be helpful in providing correct data to users and guide them concerning variant conditions on the road. The VANET applications are termed as a very important answer for the safety of the users on the road. Furthermore it's believed that the vehicular applications should be secured. As a result of the users are directly affected just in case the attackers modification the content of safety applications. Attackers modification their offensive behavior and that they launch completely different attacks at different times. Attackers continuously attempt to tamper the knowledge and make troubles within the network. the extent of trust develops within the network if the system is ready to manage attackers from distracting the data. Crypto graphical functional components are thought of as one of key parts for trust building and maintaining knowledge integrity within the past analysis work done. In future we might be addressing some attestation scheme for developing a secure and trustworthy environment in vehicular network.

REFERENCES

[1] Y.Qian, K.Lu and N.Moayeri, 2008, -A secure vanet Mac protocol for DSRC applications", Gobal Telecommunications Conference, IEEE, pp.1-5
[2] U.F.Minhas,J.Zhang,T.Tran, and R,Cohen, 2010,—Towards expanded trust management for agents in vehicular ad-hoc networks,‖ In International Journal of Computational Intelligence: Theory and Practice (IJCITP), vol. 5, no.1.
[3] Rahman, S.U. and Hengartner, U., 2007,—Secure crash reporting in vehicular Ad hoc networks‖. Proc. 3rd Intl. Conf. On Security and Privacy In Communications Networks. IEEE Computer Society, pp.443-452.
[4] W. Xiang, Y. Huang and S. Majhi, "The Design of a Wireless Access For Vehicular Environment (WAVE) Prototype for Intelligent Transportation System (ITS) and Vehicular Infrastructure Integration (VII)", Vehicular Technological Conference, (VTC-Fall), 2008
[5] Ujwal Parmar, Sharanjit Singh- "Overview of Various Attacks in VANET" International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015 ISSN 2091-2730
[6] D.Jiang,V.Taliwal, A.Meier, W.Holfelder and R.Herrtwich,"Design of 5.9GHz DSRC based vehicular safety communication", IEEE Wireless Communication Magazine, Vol 13, No.05 Nov 2006.
[7] T.Leinmuller, E. Schoch, F. Kargl, C. Maihofer, "Improved security in Geographic ad hoc routing through autonomous Position Verification", ULM University.
[8] Irshad Ahmed SumraTrust and Trusted Computing in VANET Computer Science Journal Volume 1, Issue 1, April 2011
[9] Parul Tyagi & Deepak Dembla "A Taxonomy of Security Attacks and Issues in Vehicular Ad-Hoc Networks (VANETs)" International Journal of Computer Applications (0975 – 8887) Volume 91 – No.7, April 2014
[10] Rizwanul Karim SakibSECURITY ISSUES IN VANET Department of Electronics and Communication Engineering April 16, 2010 BRAC University, Dhaka, Bangladesh
[11] Jie Zhang A Survey on Trust Management for VANETs 2011 International Conference on Advanced Information Networking and Applications © 2011 IEEE DOI 10.1109/AINA.2011.86
[12] Pankaj Singh Chouhan , Brajesh K. Shrivash , Priya Pathak "Direct Security Approach Based on Trust Management In VANET" International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 3, May-June 2015
[13] Merrihan Badr Monir, Mohammed Hashem Abd El Aziz, Ayman Adel Abdel Hamid "A Trust-Based Message Reporting Scheme For VANET" International Journal of Emerging Technology and Advanced Engineering Volume 3, Issue 5, May 2013)
[14] I.Ahmed Sumra, H.Hasbullah, I.Ahmad, and J.Bin Ab Manan, 2011,— Forming vehicular web of trust in vanet‖, Electronics, Communications and Photonics Conference (SIECPC), IEEE, pp.1-6.
[15] I.Ahmed Sumra, H.Hasbullah, I.Ahmad, and J.Bin Ab Manan, 2011,— New card based scheme to ensure security and trust in vehicular communications‖, Electronics, Communications and Photonics Conference (SIECPC), IEEE, pp.1-6.
[16] S.Biswas, J.Misic, and V.Misisc, 2011,—ID-based safety message authentication for security and trust in vehicular networks‖, Proceeding in International Conference on Distributed Computing Systems Workshops, IEEE, pp.323-331.
[17] Wenjie Wang, Tao Luo, Ying Hu They propose a novel routing protocol in city V ANET named Landmark-based routing using global real-time traffic (LRRT), 2016 2nd IEEE International Conference on Computer and Communications.
[18] Zubair Amjad "Context Aware Data Aggregation in Vehicular Ad-hoc Networks" 2016 IEEE Asia-Pacific Conference on Applied Electromagnetics (APACE) 11 - 13 December 2016 at Langkawi, Kedah, Malaysia
[19] J.Zhang, 2011,—A survey on trust management for vanets‖ In International Conference on Advanced Information Networking and Applications, pp.105-112.
[20] Ranjitha. P Securable Message Authentication System in Vehicular Ad Hoc Networks by using Trusted Authority International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.