ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

Securing Vehicular Communication through Trust Management Scheme in VANETS

K. Kalyan Kumar, M.Vijaya Kanth M.Tech,(Ph.D)

M.Tech, Department of CSE, JNTUA College of Engineering Ananthapramu, Andhra Pradesh, India

Lecturer, Department of CSE, JNTUA College of Engineering Ananthapramu, Andhra Pradesh, India

ABSTRACT: Vehicular ad hoc networks are a kind of mobile ad hoc network in which vehicles deed as nodes and these nodes are arranged with sensors in order to provide timely traffic conditions and effective reports on vehicular accidents, due to the increase of malevolent nodes trust worthiness is decreased trustworthiness can be improved through data and node trust. In order to increase data and node trust we are advising trust management scheme through which we can detect malevolent nodes and this trust Management scheme provides certificate for all authorized nodes depending upon their previous behavior through which we can eliminate malevolent nodes in VANETS

KEYWORDS: Vehicular ad hoc network, trustworthy, behavior –based, security, malevolent.

I. INTRODUCTION

In recent years Vehicular ad hoc networks have become one of the immense technology because of its unique features such as wireless communication capability and safe transportation. Vehicular adhoc networks are kind of mobile ad hoc network which do need any infrastructure and connections in mobile adhoc networks in happens wirelessly. VANET changes every engage in vehicle into wireless router, allowing vehicles to connect each other roughly up to 300 meters and form a network with a wide range. As vehicles get out of the signal range and drop out of the network, other vehicle can join the vehicles to one another in order to form a mobile network. In VANETS vehicles are dispose with sensors which gives effective information about the traffic conditions as shown in *fig. 1* and saves travelers time by making them opt to another route they also provide timely updates regarding accident prone regions, the primary objective of VANETS is to establish wireless communications among the moving nodes and also to provide on road entertainment. However the prevailing issue with VANET is the range of the wireless sensors on vehicles is confined to few hundred meters due to this we can't asses traffic conditions accurately in urban environment due to change of its dynamic topology and another problem faced by VANET is unstructured roads, the variations in the sizes of the crossway in a certain area, the sharp curves of the roads, bumpy slopes, and other complication such as large buildings, traffic lights, trees, and sign boards.

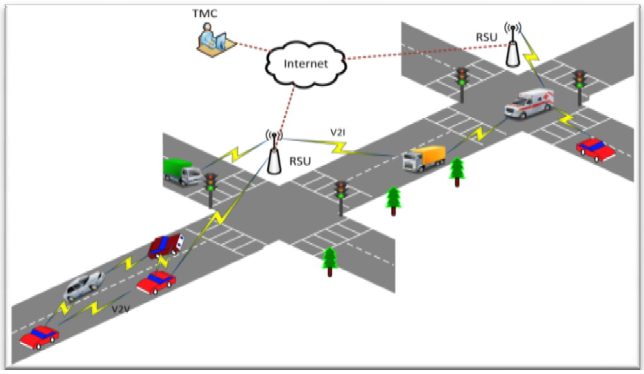

Fig: 1 vanet architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

As stated VANET architectures can be of three types namely the Wireless Wide Area Network in which cellular gateways are fixed to allow explicit communication between the access points and the vehicles, which require costly installation. Hybrid Wireless Architecture is another type of architecture in which WWAN access points are used at certain points where an ad hoc communication furnish access and communication among those access points. And the final category is node to node or node to infrastructure which does not require any fixed access points by making use of VANETS we can reduce fuel consumption and death rates they also provide information about nearby places like petrol filling stations, parking places, resorts, hospitals etc. One major complication with VANETS is trustworthiness that is whether the reported traffic data is faultless or not. When correlate with the traditional wired network.

VANETS are more accessible to malicious attacks because of their unique attributes, like Limited power, Error prone transmission and dynamic network topology. VANET technology can be applied for one city, many cities or for countries because it is geographically boundless and being an ad hoc in nature exchange of information from bordering node will be done regularly, nodes in VANET should be guarded physically so that it will be a difficult task to perform an attack on infrastructure In VANETS trust worthiness can be assessed through Data and Node trust where Data trust is defined whether the proclaimed traffic data is trustworthy or not and Node trust is defined as how reliable are the nodes in VANETS. In VANETS various nodes and roadside units are accoutered with sensors through which we can get traffic data. VANETS also help in data sharing among the nodes in the same network in order to provide above services VANETS are provided with GPS system through which we can send the updates regarding the current conditions.

II. LITERATURE SURVEY

According to J.-Y. LeBoudee and S. Buchegger misbehavior generally refers to anomalous behavior that vary from the set of behaviors that each node originally supposed to perform in ad hoc networks According to P.-W. Yau and C. J. Mitchell classify impropriety nodes in ad hoc networks as four types namely badly failed node behavior, failed node behavior, selfish attacks, and malicious attacks. These four types of impropriety nodes are categorize with respect to the node's intent and action. More specifically, selfish attacks are purpose full passive misbehaviors, where nodes will not to fully participate in the packet forwarding functionality to preserve their resources like battery power consumption; malicious attacks are designful active misbehavior, where the malicious node purposes fully halt network operations. This presence of selfishness and malicious behavior has inspired research in the area of misbehavior detection for mobile ad hoc network. There are some other attacks which mainly focus on transmission of data which is distributed in ad hoc network and one more goal of misbehavior detection is to make sure that the data is being changed while transmission that is both send and received data should be same at the receiving node.

Y. Zhang and W. Lee, proposed Intrusion detection System which is used to detecting diverse node misbehaviors in ad hoc network Due to absence of fixed infrastructure plenty of methods have been proposed to build IDS probes and in each node it is fixed with IDS probe through which there will be continues monitoring of the network traffic will leads to inefficient energy due to finite battery power for each node in MANET. Cooperative intrusion detection framework was proposed by Huang *etl* in which clusters are formed and nodes in each cluster perform the IDS task through which it power consumption is reduced in every node routing misbehavior is another security issue which is studied in ad hoc network in order to compromise some part or entire part of network some adversary is intruded into the ad hoc network .Marti *et al.* Introduced two relevant techniques, namely watchdog and path rater, in order detect and segregate misbehaving nodes, which don't forward packets. There are also some other solutions that aim to endure with discrete routing misbehaviors As VANET is a wireless network associated with different computing device deployed in vehicles requires continues monitoring in order to share current conditions

The aim of trust management is to appraise discrete behaviors of other nodes and build a prominence for each node based on behavior assessment. These appraise can be used to determine trustworthiness for other nodes, make a opinion on which nodes to cooperate with, and node to punish if it seems an untrustworthy. J.Y. L Boudec and S.Buchegger make use of Trust management system to evaluate the node behaviors. Which is of two kinds .The first

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

kind is named as first-hand observation, or directs observation First hand observation is directly made by the node itself and first hand observation can either passive or active? If the node observes its neighbor actions immorally then information which is obtained locally is known as passive. Adjacent to that it will take some evidences from reputation management system basing on the nodes previous behavior like packet acknowledgement while route exploration process where second hand observation is procure from inverting of the first hand observation with other nodes in network and primary disability of second hand observation are collisions, false report and overhead related.

CONFIDANT (Cooperation of Nodes Fairness in Dynamic Ad hoc Networks) is a proposed by Buchegger *et al* in order to reassure node cooperation and abuse misbehaving nodes CONFIDANT consists of four parts in each node, monitor, Reputation System, a Trust Manager, and a Path Manager. Where monitor inspect and find unusual routing behavior node in ad hoc network. Reputation System enumerates the reputation for each node in according to its previous behavior. Trust Manager inter change alerts with other trust managers concerning node misbehaviors. Path Manager maintains path rankings, and sends proper response to various routing messages. Some of probable drawbacks of CONFIDANT are the attacker may purposely spread false messages to other nodes saying that node is behaving even though it is well behaving

Michiardi *et al* proposed CORE which is used to find selfish nodes, and then impel them to cooperate in routing activities. Similar to CONFIDANT, CORE uses both Surveillance system and Reputation system to inspect and assess node behaviors, while CONFIDANT allows nodes to change both positive and negative observations of their neighbors, from the obtained observations only positive observations are exchanged among the nodes in CORE through which malicious nodes cannot spread fake messages to frame the well-behaved nodes, and continuously avoid denial of service attacks toward the well-behaved nodes. The reputation system manages prominence for each node, and the reputations are adjusted upon receiving of new evidences. Since selfish nodes reject to cooperate in some cases, their reputations are lower than other nodes. To encourage node cooperation and punish selfishness, if a node with low reputation sends a routing request, then the request will be ignored and the bad reputation node can't use the network.

Patwardhan *et al* proposed an approach through which the character of a node is determined by data validation. In this approach some nodes are treated as anchor nodes which are pre authenticated so that we consider the data provided by these nodes is trustworthy. Data is endorsed either by agreement among peers or direct communication with an anchor node. Malicious node can be identified if data sent is invalidated by the validation algorithm. In addition to that there are some research areas which aim to enhance the security, trust and privacy of VANET. Most of the existing trust management methods for ad hoc networks mainly target on appraise of trustworthiness of mobile nodes by collecting different evidences and analyzing the behavioral history of the nodes.

III. PROBLEM DEFINITION

VANETS are generally formed with disparate sensors which required continues observation in order to share the traffic conditions roadside units are presumed are as trustworthy as they are exceptionally protected but connected nodes are more manageable to different attacks they can be compromised at any point of time. The contender may be outsider or can be within the network it is the first which is going to compromise one or more nodes and later behave as if it's an insider this contender have the capability of modifying the results send by nodes and send fake results to the nodes in the network . The main intent of contender is to obstruct the normal data flow or to modify the data. In order to solve above problem they have made use of attack resistant trust management scheme which have the capability to cope will different types of malicious attacks.

VANETS treat every vehicle in the network as a node and these nodes are made to connect in order to form a network. In VANETS we use ART scheme in order to calculate trustworthiness among the nodes trustworthiness can be calculated by using data and node trust where data trust is used to determine if the proclaim traffic data is appropriate or not and node trust illustrate how realistic the nodes in the VANETS are. In ART node trust is examined in two different dimensions i.e. functional and recommendation trust where functional trust is defined as how fairly a node can accomplish its performance and recommendation trust is defined as how sensible the support from one node to other node will be .

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

ART scheme is constitute in two stages analysis of data and trust management, In we collect analysis of data from different nodes in network and these collected data is analyzed through a process called evidence combination in this data collected from two different nodes (n1, n2) are combined together and from the obtained result, similar results are selected and we consider theses result to be accurate these accurate results are send to the nodes in order revel the current traffic conditions. The results which are dissimilar are considered to be fake and the corresponding node is treated as mock node and action is taken towards the node. In order to collect the accurate we take one fix node that is road side unit and moving node into survey. As we know trust management is calculated by both data and node trust as shown in the *fig: 2*

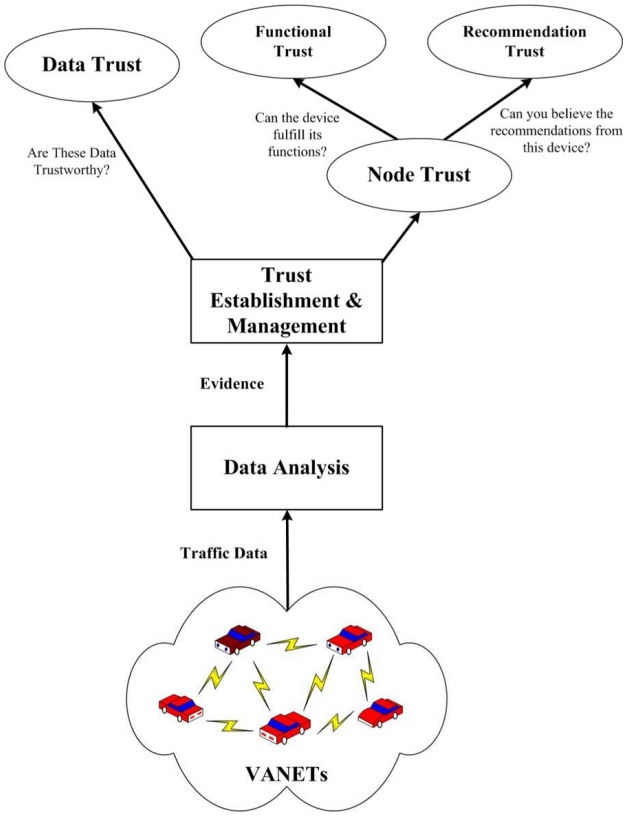

Fig: 2 node and data trust

IV. PROPOSED SYSTEM

As stated VANETS are suffering from a problem of data and node trust Due this the false reports and continues collisions are happening so that providing accurate results regarding traffic updates has became a challenging task. So, in order to fix this problem we are proposing a Certificate-based or behaviour based approach in which we provide certificates for nodes which are entering into the network these certificate is assigned to the node basing on its previous behaviour. In order to record an accurate data we take two different nodes into survey that is road side unit and moving node and results from these two nodes are recorded and certificate is provided basing on the results which obtained from evidence combination which is show in the figure 3.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

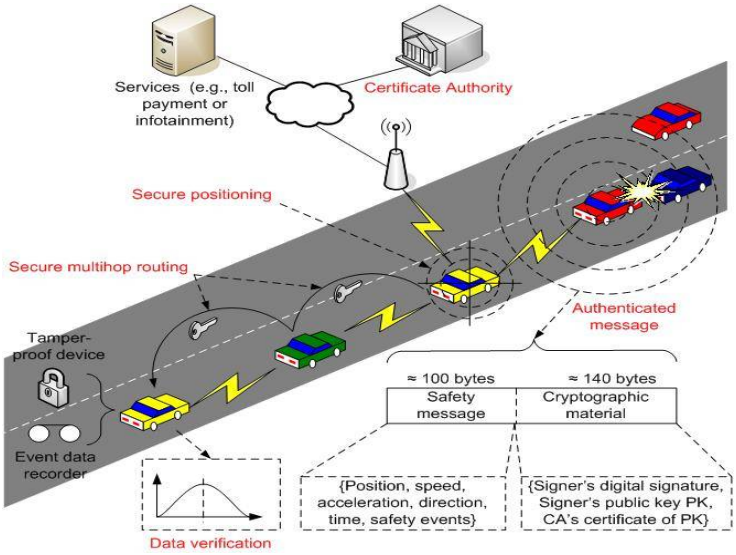

Fig: 3 certificate allocation

In the above *fig:3* its is clearly show the certificate allocation process to the nodes in the network in order establishing a secure communication among the nodes this certificate allocation is done basing on the nodes previous behavior some extensive experiments have been conducted and the results says the process can defend against various malicious attacks.

REFERENCES

1. R. G. Engoulou, M. Bellache, S. Pierre, and A. Quintero, "VANET security surveys," *Comput Commun.*, vol. 44, pp. 1–13, May 2014.
2. B. T. Sharef, R. A. Alsaqour, and M. Ismail, "Vehicular communication ad hoc routing protocols: A survey" *J. Net Comput. Appl.*, vol. 40,pp. 363–396, Apr. 2014.
3. M. Raya and J.-P. Hubaux, Securing vehicular ad hoc networks, *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007
4. M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1,no. 2, pp. 53–66, Apr. 2014.
5. M. Kakkasageri and S. Manvi, "Information management in vehicular ad hoc networks: A review," *J. Netw. Comput. Appl.*, vol. 39, pp. 334–350,Mar. 2014.
6. J. Molina-Gil, P.Caballero-Gil, and C. Caballero-Gil, "Aggregation and probabilistic verification for data authentication in VANETs," *Inf. Sci.*, vol. 262, pp. 172–189, Mar. 2014.
7. Y. Lin and H. Song, "DynaCHINA: Real-time traffic estimation and prediction," *IEEE PervasiveComput.*, vol. 5, no. 4, pp. 65–65, Oct.–Dec. 2006.
8. Caballero-Gil, C. Caballero-Gil, J. Molina-Gil, C. Hernández-Goya, Flexible authentication in vehicular ad hoc networks, Proceedings of the 15th Asia-Pacific Conf. Communications, 2009, pp. 576–879.
9. P. Michiardi and R. Molva, CORE: A Collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks" in *Proa. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Security*, Portoro˘z, Slovenia, 2002, pp. 107–121.
10.A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. 3rd Annu. Int. Conf. Mobiquitous Syst. Workshops*, Jul. 2006, pp. 1–8.
11.P. Resnick N. Iacovou, M. Suchak, P Bergstrom, and J. Riedl, "Group- Lens: An open architecture for collaborative filtering of Netnews" in *Proc. ACM Conf.*, 1994, pp. 175–186.
12. J. Davis and M. Goadrich, "The relationship between precision–recall and ROC curves," in *Proc. ACM 23rd Int. Conf. Mach. Learn.*, 2006, pp. 233–240.
13.S. Buchegger and J.-Y. L. Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," in *Proc. WiOpt, Model. Mobile, Ad Hoc Netw.*, 2003, pp. 131–140.
14.P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Proc. IFIP TC6/TC11 6th Joint Working Conf. Commun. Multimedia Security*, Portoro˘z, Slovenia, 2002, pp. 107–121.