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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

A Review on Evaluation of Security Threats in Vehicular Ad hoc Network

Richa Rani[1], Kamaljeet Kaur Mangat[2]

M.Tech Student, Dept. of CSE, Punjabi University Regional Centre for Information Technology and Management, Mohali, India[1]

Assistant Professor, Dept. of CSE, Punjabi University Regional Centre for Information Technology and Management, Mohali, India[2]

ABSTRACT: Vehicular Ad hoc Networks (VANETs) are the promising approach to provide safe wireless communication between the vehicles which becomes a key component of the intelligent transport system. VANET normally refers to a wireless network of mixed sensors or other computing devices that are deployed in vehicles. The challenges posed by vanet include storage competencies,energy restriction,peer to peer secure transmission and system accuracy. The accuracy of the system can be improved by finding the trustworthy nodes which defines the assessment of wheather or not,and upto what extent ,the reported traffic nodes are trustworthy,when the number of vehicles increased. This paper reviews the traffic and trust management system based on optimization system is proposed for VANETs that is able to find the trustworthy nodes to perform secure routing. The effectiveness and efficiency of proposed traffic and trust management system is validated through extensive experiments. The proposed management system is applicable to wide range of VANET applications to improve storage power , security , accuracy with enhanced trustworthiness.

KEYWORDS: Vehicular Ad hoc Network , VARS, Security Threats etc.

I. Introduction

VANETs were designated for the study because, among the vehicular networks, the ad-hoc configuration has the greater probable of widespread use[1]. VANET normally refers to a wireless network of mixed sensors or other computing devices that are deployed in vehicles[2]. This type of network enables constant monitoring and sharing of road situations and status of the transportation systems. Every node in VANETs is equipped with the same wireless communication interface. The nodes are restricted in energy as well as computational and storage competencies.[1] The road side units are assumed to be trustworthy since they are frequently better protected [4]. The related vehicles, on the other hand, are commonly more susceptible to various attacks,and they can be co-operated at any time after the VANET is formed[5].

Vehicular networks permit cars to communicate with each other and with a distinct infrastructure on the road. Infrastructures can be purely ad hoc between cars or facilitated by making use of an infrastructure. The organization typically consists of a set of so called roadside units that are connected to each other or even to the Internet. Otherwise, remaining infrastructure such as cellular networks can be used for this resolve. VANETs pave the way for claims ranging from real time traffic information for dynamic route optimization and accident deterrence to location dependent services, such as information on local points of interest, and entertaining[7]. The last grouping includes download of media files or web content at motionless servers such as gas stations conversation of content with other cars, or distributing content in a delay tolerant network of cars [3]. VANET requests differ in their supplies of timely message delivery. They can be real time in follow up coincidence prevention in the immediate district of an accident or difficulties on the road, accepting of small delays for the submission of route optimization, or they can be non-critical in the delay tolerant performing scenarios.

DOI: 10.15680/IJIRCCE.2016. 0406289

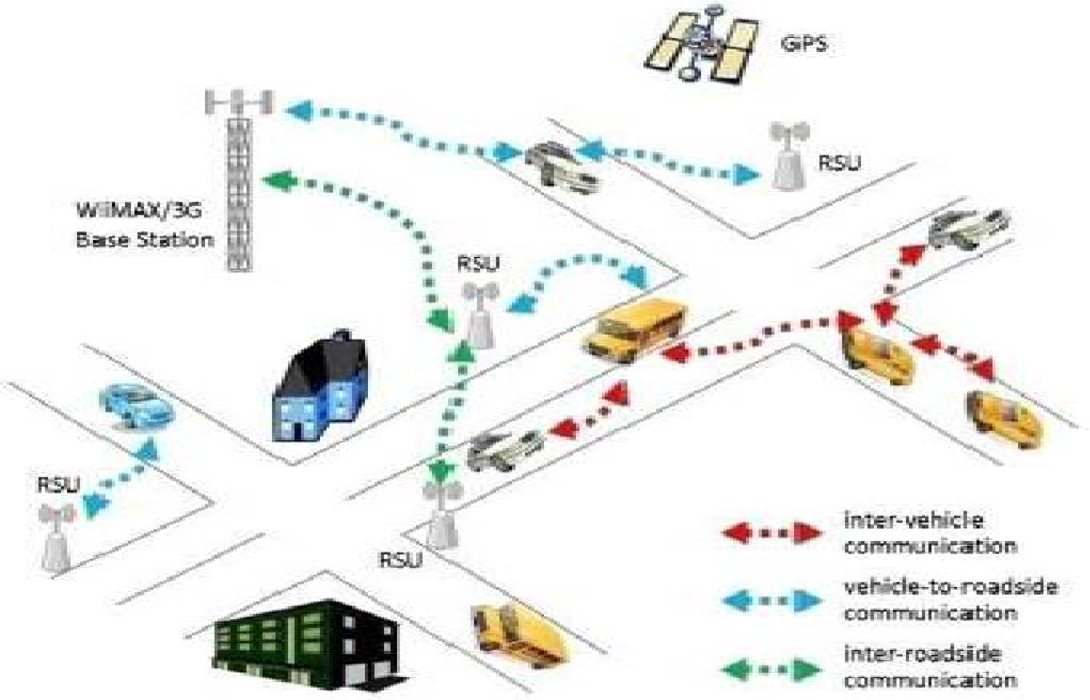
GPS
RSU
WiMAX/3G
Base Station
RSU
RSU
RSU
inter-vehicle communication
vehicle-to-roadside communication
inter-roadside communication

Fig. 1 VANET architecture [6]

Trust Management System in VANET

First of all, the vehicles in a VANET are constantly roaming around and are highly dynamic. On a typical highway the average speed of a vehicle is about 100 kilometers an hour[7]. At high speeds the time to react to an imminent situation is very critical, therefore, it is very important for the peers to be able to verify/trust incoming information in real-time. Second, the number of peers in VANET can become very large.

The major assistances of the work are listed as follows:

- First, an attack resistant trust management arrangement is studied, which can efficiently detect and cope with dissimilar types of malicious behaviors in VANETs.
- Second, the reliability of traffic data (data trust) is appraised based on the data sensed and collected from multiple vehicles .
- Third, the trustworthiness of vehicle nodes is measured in two dimensions.

In other words, a vector that is collected of two elements is used to designate the trustworthiness of each node. The two dimensions of node trust are efficient trust and reference trust,which designate how likely a node can fulfill its functionality and how trustworthy the commendations from a node for other nodes will be, individually[2].

- Finally, widespread experiments have been shown, and untriedconsequences show that the proposed ART scheme can effectually evaluate the trustworthiness set both sensed data and mobile nodes in VANETs.

II. Related work

In [1] Authors describes the an attack-resistant trust management scheme is future for VANETs that is able to notice and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. particularly, data trust is evaluated based on the data sensed and composed from multiple vehicles; node trust is assessed in two size, i.e., functional trust and suggestion trust, which indicate how likely a node can fulfill its

DOI: 10.15680/IJIRCCE.2016. 0406289

functionality and how trustworthy the recommendation from a node for other nodes will be, correspondingly.The trustworthiness of VANETs could be better by addressing holistically both data trust, which is defined as the appraisal of whether or not and to what extent the report traffic data are dependable, and node trust, which is defined as how dependable the nodes in VANETs are. The usefulness and efficiency of the future ART scheme is validated through widespread experiments.

In [6] Author provides an overview dealing with all the issues facing VANET, in particular, VANETs characteristics that distinguish them from other types of ad hoc networks, VANET system architecture focusing on different network layers with various architectural models proposed by different authors, VANET applications both for safety and entertainment purposes and finally some VANET open research areas are discussed that still need to be addressed in order to enable the deployment of VANET technologies, infrastructures, and services cost-effectively, securely, and reliably. There are a number of contributions that produced significant results, but the general feeling is that the subject is not still mature, and that a lot of work remains to be done. It is expected that this paper will help students, developers and researchers to address the challenges involved in VANET.

In [7] Author descibes the concept of VANET by considering a shortened mobility model that captures the result of hot areas in the city, we severely prove that common traffic entries, where large volume of traffic touches, play a major role in generating the exponential tail of the intercontact time. Our outcomes thus provide essentialprocedures on design of new vehicular mobility models in urban situations, new data forwarding protocols and their presentation analysis.

In [8] The security games projected for vehicular networks take as an input importance measures computed by planning the significance values of the car networks to the primary road topology. The resulting strategies help localizing most valuable or susceptiblepoints in vehicular networks.

In [9] Author discovered the fact that the unique characteristics of group signature, which is an important cryptographic ancient, perfectly match the security and privacy requirements in VANETs. By taking different security and privacy requirements of two types of VANET communications into account, namely, vehicle-to-infrastructure and vehicle-to-vehicle infrastructure, they propose a novel secure and privacy-preserving protocol for vehicular communication, based on a grouping of group signature and identity based signature techniques.

In [10] A modular standing system architecture that strictly separate shortest and indirect reputation handling from opinion generation. VARS is not based on the performance of nodes but on the estimation about distributed content, i.e., forwarding nodes form estimation on the satisfied of a message; this opinion is attached to the message before forwarding it to other nodes. Therefore, receiver can appraise the opinion of other nodes and use it as a basis for their own decision about the trustworthiness of a message. On entrance of an event communication every forwarding node generates an opinion on the trustworthiness of this message. An opinion is calculated from experience if the event is detected, from indirect trust if the sender is known, or from incomplete opinions attached to the message or a grouping thereof.

III. Conclusion and future work

In the survey, it has concluded that each node in VANET is restricted in energy as well as computational and have storage competencies [1] because every node is equipped with the same wireless communication interface. To overcome the issue of restricted energy and storage competencies an optimization scheme that is Particle Swarm Optimization has been implemented for traffic and trust management system. In Future scope, the implementation of existing defence approaches can be used in broader range of apllication scenerio. Thus, it will make vehicular ad-hoc network more resistant to security attacks.

References

1. Wenjia Li, and Houbing Song, "*ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks*", IEEE Transaction on intelligent transportation systems ,vol.17, no. 4, pp. 960-969, 2015

2. Vinh Hoa LA, Ana CAVALLI, "*Security Attacks and Solutions in Vehicular Ad hoc Nwtworks*", International Journal on AdHoc Networking Systems , Vol. 4, no. 2, pp. 356-368, 2014

3. R. G. Engoulou, M. Bellache, ST. Pierre, and A. Quintero, "*VANET security surveys," Comput. Communication.*, vol. 44, no. 0, pp. 1–13, 2014.

4. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "*A comprehensive survey on vehicular ad hoc network*," J. Networks Computer Application, vol. 37, no. 1, pp. 380–392, 2014.

5. Ankita Agrawal, Aditi Garg, Niharika Chaudhiri, " *Security on Vehicular Ad Hoc Networks (VANET),"* International Journal of Emerging Technology and Advanced Engineering , vol 3, no. 1, pp. 2250-2459, 2013

6. Md. Humayun Kabir, "*Research Issues on Vehicular Ad hoc Network",* International Journal of Engineering Trends and Technology, vol. 6, no. 4, pp. 231-381, dec 2013.

7. Zhu, Hongzhi, "*Impact of traffic influxes: Revealing exponential intercontact time in urban vanet.*", IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 8, pp. 1258-1266, 2011

8. Alpcan,Tansu and Sonja Buchegger, "*Security games for vehicular network.*", IEEE Transactions on mobile computing, vol. 10, no. 2, pp. 280-290, 2011

9. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS*: A secure and privacy preserving protocol for vehicular communications*," IEEE Transaction Vehicular Technology, vol. 56, no. 6, pp. 3442–3456, 2007

10. Dotzer F, Fischer L, Magiera P, "*Vars: a vehicle ad-hoc network reputation system*", IEEE international symposium on a world of wireless mobile and multimedia networks, vol. 34, no. 8, pp. 454–456, 2005