ISSN : 2455-9679
Impact Factor : 2.865

IJRTSM

INTERNATIONAL JOURNAL OF RECENT TECHNOLOGY SCIENCE & MANAGEMENT

"TRUST MANAGEMENT SCHEME FOR VEHICULAR AD-HOC NETWORK SECURITY: A SURVEY"

Yuvika Ahuja [1], Prof. Deepak rathore [2]

[1] *M.Tech. Scholar, Dept. of CSE, LNCT Bhopal, Mp, India*

[2] *Associate Professor, Dept. of CSE, LNCT Bhopal, Mp, India*

ABSTRACT

In recent years, due to the rapid growth of new technologies in Internet communication, ultra-connected world has become a strategic element. In the current era of ubiquitous connectivity, wireless communication technologies have enabled a kaleidoscopic range of applications that are revolutionizing many aspects of business and public services. In this article we present the survey for the broadcast scheme and medium access control layer protocol in the vehicular ad-hoc network. We also discuss about the challenges or issues regarding the key management and privacy of the data.

Keyword: *Vehicular ad hoc networks, Medium Access Control, Time Division Multiple Access (TDMA), end to end Delay, Trust value*

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is poised to offer the drivers and passengers with a safe, at least fail safe, reliable, and infotainment rich driving environment. From the research results in the field of vehicular networks (semiautonomous) and driverless (autonomous) cars, it can be easily speculated that intelligent transportation system (ITS) technologies, which are realized through VANET, will be soon pervading our highways [3]. Ad-Hoc networks have grown in a thick and fast way as result of increased need of eliminating fixed infrastructure, geographical dependence and complexity of deployment for critical applications such as Industrial IoT (IIoT), military operations, disaster relief management, maritime communications, intelligent transportation systems, wild-life monitoring, health monitoring and many more. A Mobile Ad-hoc Network (MANET) is such an autonomous distributed network of mobile nodes which supports wireless communication in decentralized environment with geographical independence and impulsive deployment.

A mobile ad-hoc cloud is formed from such a MANET which inherits the merits of cloud computing paradigm such as flexibility, efficient resource utilization and enhanced manageability. It provides services by exploiting the available computing resources in the mobile nodes [2].

The mobility patterns, based on space and time, are predictable in VANET and linked to online social networks (OSNs). For example, the traffic tends to be dense during rush hours because people are going to office in the morning and coming back home in the evening, which is not the case for non-peak hours. This phenomena develops a unique social relationships among neighbors who tend to share same interests and/or likely schedule. The recent developments in OSNs gives rise to the concept of VSN by providing a preferred mean of sharing social activities among VANET users. Consequently, many VSN applications are developed for this purpose such as Tweeting car, Social Drive, Social

ISSN : 2455-9679
Impact Factor : 2.865

based navigation (NaviTweet), Clique Trip, and Geo Vanet. Beside the technological advancements, it is essential to look at the social perspective of VANET [3].

Vehicular Ad-hoc Networks (VANETs) have tremendous potential to improve vehicle and road safety, traffic flow efficiency, and convenience since enabling the information dissemination between vehicle-to-vehicle (V2V) and vehicle to infrastructures (V2I). VANETs are characterized differently from the traditional wired network by the quick movement, unreliable channel, and short-lived link. These characteristics emphasize the context-aware ability to handle the right information using the appropriate ways at the proper time, and also pose many security protection challenges. Since the medium is open in VANETs, appropriate security mechanism is a must on the top list of priority before extensive deployment. Many efforts have been made in countermeasures against malicious attacks and improvements of security defense, e.g., authentication, integrity, and non repudiation [4].

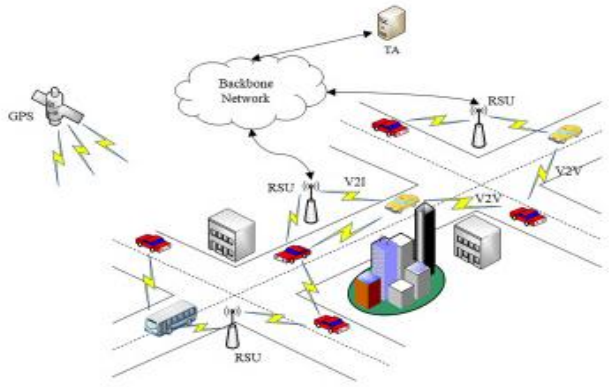

Figure 1: Network structure [5]

The applications of VANETs are classified into two classes. One is the critical class, which includes the human life on priority [6]. It covers the following: diversion notification, response to an emergency event, lane handling, congestion minimization or avoidance, information of road conditions, prioritizing to the emergency vehicles like medical van and fire truck. The second class is add-on services like navigation and payment at toll barrier. As VANET handles the core domain of intelligent transportation system so security is the major concern in such systems, where any security breach can affect its performance. Security of VANETs may have various challenges with respect to new and emerging threats such as zero-day attacks, spoofing, man-in-the middle, etc. Such types of networks are highly sensitive data privacy and type of information exchanges. Hence, they require attention before their final implementation in any application. man-in-the middle, etc. Such types of networks are highly sensitive data privacy and type of information exchanges. Hence, they require attention before their final implementation in any application. For example, suppose, naive moving nodes (vehicles), as shown in below figure.

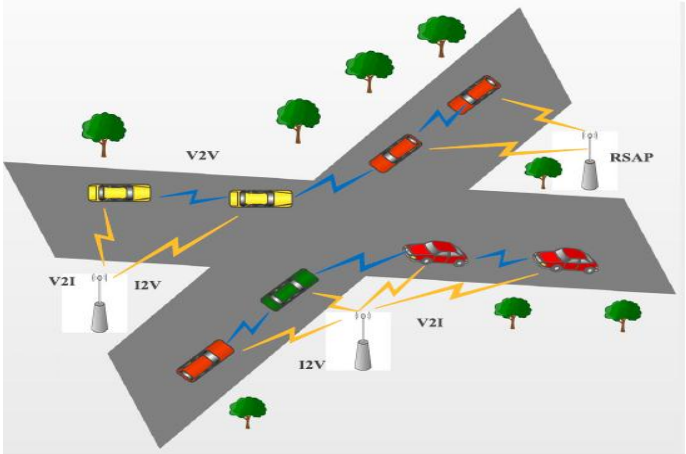

Figure 2: Basic model of VANET

ISSN : 2455-9679
Impact Factor : 2.865

The rest of this paper is organized as follows in the first section we describe an introduction of about Vehicular ad-hoc networks and Mac Protocol. In section II we discuss about the Vanet applications. in section III we discuss about the technology for the various communication protocol. In section IV we discuss about the rich literature survey for the Medium Access Control layer protocol and the vehicular ad-hoc network security issues, finally in section V we conclude the about our paper which is based on the literature survey and specify the future scope.

II. VANET APPLICATIONS

Recently, various solutions have been proposed to achieve security in VANET. Most of these solutions rely on traditional cryptography where vehicles utilize certificates and Public Key Infrastructure (PKI) to ensure security in the network. However, cryptography-based solutions reduce network efficiency due to following reasons. (1) Firstly, VANET includes both low and highly mobile vehicles which are dispersed randomly throughout the network, (2) Secondly, presence of an infrastructure cannot be ensured permanently, e.g., in rural areas, and (3) lastly, cryptographic solutions can be compromised by insider attacks in VANET, which results in the propagation of un trusted messages across the network. In order to address these shortcomings, trust has been proposed as a relevant technique to achieve network security. Trust is defined as the confidence of one node on the other for performing a specific action or set of actions [7]. In VANET, it is established between two vehicles based on the messages exchanged regarding an event. Once, message is received, the evaluator node calculates trust based on numerous factors, including vehicles past interactions, vehicles reputation in the network and neighbors' recommendations about particular vehicle.

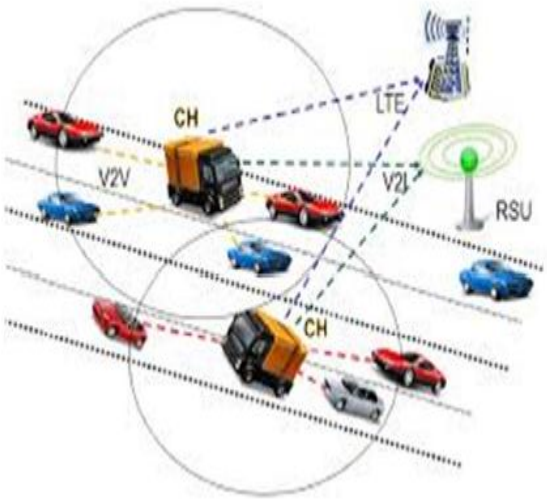

Figure 3: Illustration of VANET.

III. TECHNOLOGIES FOR COMMUNICATIONS

The connected cars have multiple communication possibilities to connect to external networks and services. A model that clarifies the different types of possible communication. Details of these are described in the following paragraphs. Connected vehicles is a new paradigm of Intelligent Transport Systems (ITS) that aims to improve the safety and efficiency of road traffic by using wireless communications. Communications of connected vehicles (or, V2X) encompass wireless communications between vehicles and infrastructure (V2I), between vehicle and vehicle (V2V), and between vehicles and wireless devices. Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication systems will increasing road capacity, avoiding accidents, comfort services, and other applications. The hardware architecture needed for a new-generation car includes a great number of different devices (from the ECUs controlling the behavior of the vehicle, to the man machine interface collecting the driver's input), connected one to another via dedicated buses [8]. Short range static communication. The applications in short range static

ISSN : 2455-9679
Impact Factor : 2.865

communication have become common nowadays. Connected cars applications utilize various wireless communication technologies in order to achieve a good connectivity, which is essential in ubiquitous computing.

IV. RELATED WORK

In this section we discuss about the rich literature survey for the vehicular adhoc network using medium access control layer protocol**.**

[1] In this paper, an attack-resistant trust management scheme (ART) is proposed for VANETs that is able to detect and cope with malicious attacks and also evaluate the trustworthiness of both data and mobile nodes in VANETs. Specially, data trust is evaluated based on the data sensed and collected from multiple vehicles; node trust is assessed in two dimensions, i.e., functional trust and recommendation trust, which indicate how likely a node can fulfill its functionality and how trustworthy the recommendations from a node for other nodes will be, respectively. The effectiveness and efficiency of the proposed ART scheme is validated through extensive experiments. The proposed trust management theme is applicable to a wide range of VANET applications to improve traffic safety, mobility, and environmental protection with enhanced trustworthiness.

[2] In this paper, they perform sensitivity analysis of TRS-PD which is carried out by varying values of different parameters in distinct network scenarios in the existence of three distinct packet dropping attacks. In addition, this work summarizes the attack-pattern discovery mechanism, trust model, and routing mechanism adopted by TRS-PD in order to counter the adversaries which follow certain attack patterns along with other adversaries. Experiments conducted with network simulator-2 indicate the correct choices of parameter values for distinct network scenarios.

[3] This paper addresses the trust management problem in the emerging Vehicular Social Network (VSN). VSN is an evolutionary integration of Vehicular Ad hoc Network (VANET) and Online Social Networks (OSN). The application domain of VSN inherits the features of its parental VANET and OSN, providing value-added services and applications to its consumers, i.e. passengers and drivers. However, the immature infrastructure of VSN is vulnerable to security and privacy threats while information sharing, and hard to realize in the mass of vehicles. Therefore, in this paper, we particularly advocate for communication trust establishment and management during information exchange in VSN.

[4] This paper views the security level as a user's inherent property that is only correlated with the user's behaviors and the situated context and independent of the suffered attack ways. They propose a formalized methodology to especially quantify the security level in real time from the perspective of state transition probability through estimating the stable probability of staying in the security state in inhomogeneous continuous time Markov chain. This paradigm enables users to customize the security protection mechanisms for adapting to the frequently varying context. They conduct the extensive numerical calculations and empirical analysis to comprehensively investigate the response of the proposed security quantification framework to the various combinations of the concerned parameters, e.g., SNR, velocity, and traffic flow.

[5] In this paper, they propose a misbehavior detection mechanism based on a support vector machine (SVM) and Dempster-Shafer theory (DST) of evidence to resist false message attack and message suppression attack. The proposed mechanism includes data trust model and vehicle trust model. The data trust model uses an SVM-based classifier to detect false messages based on message content and vehicle attributes. The vehicle trust model consists of a local vehicle trust module and a trust authority (TA) vehicle trust module. The local vehicle trust module uses another SVM-based classifier to evaluate whether the vehicle is credible based on the behavior of the vehicle in terms of message propagation. Then, the TA vehicle trust module uses DST to aggregate multiple trust assessment reports about the same vehicle and derives a comprehensive trust value. Simulation results show that Gaussian kernel best fits our models compared with other functions.

[6] In this paper provides a detailed survey on various types of attacks and possible solutions to handle these attacks. Using the proposed survey, a detailed taxonomy based upon the types of attacks and possible solutions to handle these

attacks is proposed. Finally, various emerging open issues and challenges along with the security threats are identified and discussed in the paper. These open research issues motivate the communities to design new solutions to mitigate the existing new security threats in this area.

[7] In this paper author propose a novel trust evaluation and management (TEAM) framework, which serves as a unique paradigm for the design, management, and evaluation of TMs in various contexts and in presence of malicious vehicles. Our framework incorporates an asset-based threat model and ISO-based risk assessment for the identification of attacks against critical risks. The TEAM has been built using VEINS, an open source simulation environment which incorporates SUMO traffic simulator and OMNETCC discrete event simulator. The framework created has been tested with the implementation of three types of TMs (data oriented, entity oriented, and hybrid) under four different contexts of VANET based on the mobility of both honest and malicious vehicles. Results indicate that the TEAM is effective to simulate a wide range of TMs, where the efficiency is evaluated against different quality of service and security-related criteria. Such framework may be instrumental for planning smart cities and for car manufacturers.

[8] In this article, they focus on wireless technologies and potential challenges to provide a communication's vehicle-to-vehicle(V2V) or vehicle-to-X(V2X). In particular, we discuss the challenges and review the state-of-the-art wireless solutions for internet of vehicle(IOV). Connected cars themselves as new born of new technologies, are the next frontiers for the automobile revolution and the key to the evolution towards the next generation of intelligent transport systems that enable information sharing and communication between vehicles and their internal and external environment. Moreover, connected cars are the main use cases of internet of things (IOT), yet they are the least understood in terms of cyber security. They also identify future research issues for building connected vehicles and solutions which have been proposed by several researchers.

[9] The proposed work provides man-in-the-middle attack resistance and mutual authentication using certified public key and out-of-band sense-able attributes. As the CA pre-processes every vehicles public key and unchangeable attributes, there is no way that man-in-the-middle can fake the public key or the unchangeable attributes. Also, the out-of-band attributes are sense-able and can be confirmed, while moving on the road. There is no need to communicate with the CA during the real-time session key establishment of a secret key based on the mutual authentication of vehicles. The proposed approach is simple, efficient and ready to be employed in current and future vehicular networks.

[10] In this paper, they propose an intelligent naïve Bayesian probabilistic estimation practice for traffic flow to form a stable clustering in VANET, briefly named ANTSC. The proposed scheme aims to improve routing by employing awareness of the current traffic flow as well as considering the blend of several factors, such as speed difference, direction, connectivity level, and node distance from its neighbors by using the intelligent technique. The proposed technique has proven to be more strong, stable, robust, and scalable than existing ones.

V. CONCLUSIONS AND FUTURE SCOPE

Safety as well as luxury in travel has gained significant importance in social life. For the past few decades, every year many people have lost their lives, while others have been injured in highway accidents because the driver is unable to estimate the circumstances on the road ahead. Well-organized traffic control systems are also becoming abundant. In this paper we discuss about the security issues and the medium access control for the channel using trust value.

REFERENCES

1. Wenjia Li, Houbing Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 17, NO. 4, APRIL 2016, pp 960-969.

2. RUTVIJ H. JHAVERI, NARENDRA M. PATEL, YUBIN ZHONG, AND ARUN KUMAR SANGAIAH, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT", IEEE Access 2018, pp 20085-20103.
3. Rasheed Hussain, Waqas Nawaz, JooYoung Lee, Junggab Son, and Jung Taek Seo, "A Hybrid Trust Management Framework for Vehicular Social Networks", 2016, pp 1-13.
4. X. Y. TIAN, Y. H. LIU, J. WANG, W. W. DENG, AND H. OH, "Computational Security for Context-Awareness in Vehicular Ad-Hoc Networks", IEEE 2016, pp 5268-5279.
5. CHUNHUA ZHANG , KANGQIANG CHEN, XIN ZENG, AND XIAOPING XUE, "Misbehavior Detection Based on Support Vector Machine and Dempster-Shafer Theory of Evidence in VANETs", IEEE Access, 2018. Pp 59860-59870.
6. Sudeep Tanwar, Jayneel Vora, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S. Obaidat, "A systematic review on security issues in vehicular ad hoc network", John Wiley & Sons, Ltd., 2018. Pp 1-26.
7. FARHAN AHMAD , VIRGINIA N. L. FRANQUEIRA, ASMA ADNANE, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks", IEEE Access 2018, pp 28643-28660.
8. S. Tbatou , A.Ramrami , Y. Tabii , "Security of communications in connected cars Modeling and safety assessment", Conference Paper , March 2017, pp 1-8.
9. Shlomi Dolev, Lukasz Krzywiecki, Nisha Panwar, Michael Segal, "Certificating Vehicle Public Key with Vehicle Attributes", SAFECOMP 2013, 32nd International Conference on Computer Safety, Reliability and Security, Sep 2013, pp 1-18.
10. AMJAD MEHMOOD, AKBAR KHANAN, ABDUL HAKIM H. M. MOHAMED, SAEED MAHFOOZ, HOUBING SONG, SALWANI ABDULLAH, "ANTSC: An Intelligent Naïve Bayesian Probabilistic Estimation Practice for Traffic Flow to Form Stable Clustering in VANET", IEEE Volume-6, 2018. Pp 4452-4461.
11. Sailesh Bharati, Weihua Zhuang, Lakshmi V. Thanayankizil, Fan Bai," Link-Layer Cooperation Based on Distributed TDMA MAC for Vehicular Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 66, NO. 7, JULY 2017. Pp 6415-6427.
12. Sarang C. Dhongdi, K.R. Anupama, Rohit Agrawal, Lucy J. Gudino, "Simulation and Testbed Implementation of TDMA MAC on Underwater Acoustic Sensor Network", IEEE 2016. Pp 1-6.
13. Ejaz Ahmed, Hamid Gharavi, "Cooperative Vehicular Networking: A Survey", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 19, NO. 3, MARCH 2018. Pp 996-1014.
14. Chuan Li, Hongwei Zhang, Jayanthi Rao, Le Yi Wang, George Yin, "Cyber-Physical Interference Modeling for Predictable Reliability of Inter-Vehicle Communications", 2017. Pp 1-10.
15. SairaAndleeb Gillani, Peer Azmat Shah, Amir Qayyum, Halabi B. Hasbullah, "MAC Layer Challenges and Proposed Protocols for Vehicular Adhoc Networks", 2015. Pp 1-11.
16. Ju Tan, Hongping Gan, Peng Li, " Improved MAC Protocol Based on Time Division Multiple Access In Multi Channel Vehicular Networks", Journal of Residuals Science & Technology, 2016. Pp 88.1-6.
17. Meng-yue YU, Xin YANG, "A Multi-hop MAC Protocol Based on Coordinating Relay Node", 2nd International Conference on Advances in Management Engineering and Information Technology, 2017. Pp 279-284.
18. RobertoM.Oliveira,MichelleS.P.Facin,MoisesV.Ribeiro, AlexB.Vieira, " Performance evaluationof in-home broadband PLC systems using a cooperative MAC protocol", Elsevier ltd. 2016. Pp 62-76.

ISSN : 2455-9679
Impact Factor : 2.865

19. Xin Yang, Ling Wang, Jian Xie, "Energy Efficient Cross-Layer Transmission Model for Mobile Wireless Sensor Networks", Hindawi Mobile Information Systems, 2017. Pp 1-9.
20. Rodrigo Teles Hermeto, Antoine Gallais, Fabrice Theoleyre, "Scheduling for IEEE802.15.4-TSCH and Slow Channel Hopping MAC in Low Power Industrial Wireless Networks: A Survey", 2017. Pp 1-38.
21. Omprakash Kaiwartya, Sushil Kumar, "Guaranteed Geocast Routing Protocol for Vehicular Adhoc Networks in Highway Traffic Environment", Wireless Pers Commun, Springer 2015. Pp 1-27.
22. Mahdi Zareei, A.K.M. Muzahidul Islam, Cesar Vargas-Rosales, Nafees Mansoor, Shidrokh Goudarzi, Mubashir Husain Rehmani, "Mobility-aware medium access control protocols for wireless sensor networks: A survey", Elsevier ltd. 2018. Pp 21-37.
23. Damilare Oluwole Akande, Mohd Fadzli Mohd Salleh, Festus Kehinde Ojo, "MAC protocol for cooperative networks, design challenges, and implementations: a survey", Springer 2018. Pp 1-18.