ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-4, 2019

Vehicular Ad-hoc Network for Road Safety Applications: Survey & Discussions

Navin Kumar[1], Dr. Neetesh Gupta[2]

[1]M. Tech Scholar, Department of CSE, TIT&S, Bhopal (India)

[2]Head & Professor, Department of CSE, TIT&S, Bhopal (India)

[1]navinpcst@gmail.com, [2]gupta_neetesh81@gmail.com

ABSTRACT

In the recent years, car manufacturing industries, academia and government agencies have started putting much joint efforts together towards realizing the concept of vehicular communications in wide scale. In the near future, vehicles will have the capability to communicate with each other directly in a Vehicle-to-Vehicle (V2V) manner or indirectly using the existing infrastructure alongside the road in a Vehicle-to-Infrastructure (V2I) way. This will enable the implementation of numerous Intelligent Transportation Systems (ITS) applications, including road safety, traffic efficiency and infotainment applications, assisting drivers in avoiding dangerous situations or provisioning of convenience applications for passengers. In this paper we survey for the vehicular ad-hoc network and discuss their applications for the road safety.

Keywords:- Mobile ad-hoc network, Vehicular ad-hoc network, Vehicle to vehicle, Vehicle to infrastructure, Single hop, Multi hop.

INTRODUCTION

Wireless communication and networking is a rapidly emerging technology in recent years, which regardless of geographic position allows devices to interconnect with each other. There are several types of wireless networks depending on the application, like Wireless Personal area networks (WPANs), Wireless local area networks (WLANs), Mobile ad-hoc networks (MANETs) etc. There are two types of wireless networks depending on facilities or not, infrastructure based the cellular network and infrastructure less wireless networks. In infrastructure based networks there are stationary parts, like base stations or access points to which nodes can connect, while in infrastructure less or ad hoc networks there is no fixed infrastructure and nodes communicate with each other directly, while they reside within each other's radio range (single-hop) or in-directly through other nodes (multi-hop) when they are out of the receiver's radio range.

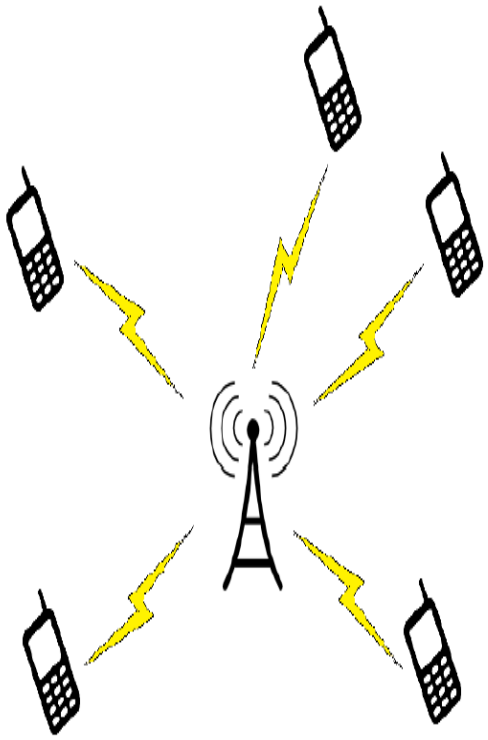

Fig 1: Infrastructure based network.

MANETs are formed by two or more devices or nodes without a central or fixed infra-structure. The term Ad Hoc states the absence of infrastructure. Because of this absence of base stations in MANETs nodes have to relay packets to reach the destination, that is to say, each node acts as a router for the neighboring nodes. The communication between nodes strongly depends on the nodes' cooperation. There is always the case of a misbehaving node to disrupt the normal reception of a packet. Such attacks will be detailed in a following chapter. A MANET is a self-organizing and self-configuring net-work with the potentiality of rapid deployment of mobile nodes forming a temporary and highly dynamic in most cases network, where nodes join or leave the network independently over time. The network could be partitioned in sub-networks, as in cluster based architecture, which is detailed below in this chapter. Nodes could move at will from a sub-network to another in the vicinity.

Increasing road accidents and vehicle traffic congestions have led to the evolution of intelligent transportation systems (ITS) [2] and other applications that improve road safety, increase transportation efficiency, and provide on-board infotainment. To make these applications possible, vehicles are equipped with sensors and communication devices such that they can gather and exchange information to maintain road safety as well as to optimize vehicle-traffic efficiency. Moreover, wireless technology makes communication among vehicles possible, forming a vehicular ad hoc network (VANET). The National Highway Traffic Safety Administration (NHTSA) of the United States Department of Transportation (USDoT) has predicted that traffic accidents, specifically vehicle collisions, can be reduced by approximately 80% through the deployment of safety applications enabled by VANETs.

The rest of this paper is organized as follows in the first section we describe an introduction of about the mobile ad-hoc network, vehicular ad-hoc network and their application. In section II we discuss about the security services in vehicular ad-hoc network, In section III we discuss about the literature survey in the vehicular ad-hoc network, finally in section IV we conclude the about our paper.

II SECURITY SERVICES OF VANET

- **Authentication:** The sender of the messages must be authenticated. Nodes should react to the information received from the legitimate users only. As an unauthorized node may transmit false information and mislead others. Therefore we need to authenticate the senders of these messages. . It is a challenging task within the vehicular network to ensure authentication because of unattended nature of the network and wireless nature of the transmission media.

- **Integrity:** The correctness and timely receipt of information is a major vulnerability. This service deals with the consistency of a stream of messages throughout communication. In the vehicular network, data Integrity is needed to ascertain the reliability of the data. It assures that messages are received as sent without insertion, modification, replays or reordering. As a vehicle can act malicious and tamper the information sent, though it may be a legitimate user.

- **Non-repudiation:** Non-repudiation service refers that either sender or receiver cannot deny the transmission of a message. It is possible that a node may transmit false traffic alerts, however later it refuses that the messages were sent by it.This service may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident [19].

- **Confidentiality:** This service ensures that the classified information in the network can never be disclosed to the illegitimate users. Confidentiality protects the privacy of the confidential communication content like name, location, plate number etc. It guarantees the privacy of drivers against unauthorized observers

[17]. Pseudonyms technique is used in order to preserve the privacy of the drivers in VANETs.

- **Availability:** There can be attacks that can lead to loss or reduction in the availability of VANET services such as bandwidth and connectivity. Even a robust communication channel can still suffer some attacks (such as denial of service) which can bring down the network [17]. Therefore, availability of VANETs resources should be also supported by alternative means so that's communication is not hampered.

- **Access Control:** In VANET, it is essential to define the access privileges for different users. The authorized party needs to define the network policies for the vehicles to access the network [12]. This will help to control the access of different users to various services provided by the VANETs. Access control can be implemented through communication channels, to limit a user's access other vehicles, applications and RSUs.

III RELATED WORK

Wireless communication and networking is a rapidly emerging technology in recent years, which regardless of geographic position allows devices to interconnect with each other. Increasing road accidents and vehicle traffic congestions have led to the evolution of intelligent transportation systems (ITS) and other applications that improve road safety, increase transportation efficiency, and provide on-board infotainment.

[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, they 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.

IV CONCLUSIONS

Wireless communications and networking is a rapidly emerging technology in recent years due to the ease of use and transportation of light weight mobile devices. Nowadays, sensor-based technologies are playing a vital role in the automation industries. In this paper we present the rich literature survey for the road safety applications using vehicular ad-hoc network, in the future we plan to implement the robust mechanism for the vehicular ad-hoc network to improve the performance of network.

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] 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", Journal of Network and Computer Applications 104 (2018) 21–37.

[7] Sudeep Tanwar, Jayneel Vora, Sudhanshu Tyagi, Neeraj Kumar, Mohammad S. Obaidat, "A systematic review on security issues in vehicular ad hoc network", Wiley 2018, pp 1-26.

[8] 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.

[9] 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.

[10] Ejaz Ahmed, Hamid Gharavi, "Cooperative Vehicular Networking: A Survey", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 19, NO. 3, MARCH 2018. Pp 996-1014.

[11] 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.

[12] SairaAndleeb Gillani, Peer Azmat Shah, Amir Qayyum, Halabi B. Hasbullah, "MAC Layer Challenges and Proposed Protocols for Vehicular Adhoc Networks", 2015. Pp 1-11.

[13] Mohamed Hadded, Paul Muhlethaler, Anis Laouiti, Rachid Zagrouba, Leila Azouz Saidane, "TDMA-based MAC Protocols for Vehicular Ad Hoc Networks A Survey, Qualitative Analysis and Open Research Issues", IEEE COMMUNICATION SURVEYS AND TUTORIALS , VOL. , NO. , FEBRUARY 2015, pp 1-36.

[14] Roberto M.Oliveiraa, Michelle S.P.Facina, Moises V.Ribeiro, AlexB.Vieira, " Performance evaluation of in-home broad band PLC systems using a cooperative MAC protocol", Computer Networks 95 (2016) 62–76.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] Omprakash Kaiwartya, Sushil Kumar, "Guaranteed Geocast Routing Protocol for Vehicular Adhoc Networks in Highway Traffic Environment", Wireless Pers Commun, Springer 2015. Pp 1-27.

[20] 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.