ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-6, 2019

A Review on Vehicle Node in Wireless Communication

Chandni Ahirwal[1], Prof. Jitendra Mishra[2]

[1]M. Tech Scholar, Department of EC, PCST, Bhopal (India)

[2]Head & Professor, Department of EC, PCST, Bhopal (India)

ABSTRACT

The field of wireless communications has been in existence since the first humans learned to communicate. The area of wireless communications will continue to grow for many reasons. People are becoming accustomed to immediate access to information wherever their locations and technological improvements have made providing universal telecommunications access feasible. Wireless communication changed the human life in drastic manner in the form of mobile ad-hoc network and vehicular ad-hoc network, in this paper we review the wireless communication for the vehicular ad-hoc network, and discuss the various issues and challenges for the current wireless communication system.

Keywords:- Wireless communication, Mobile ad-hoc network, Vehicular ad-hoc network, Wireless local area network.

INTRODUCTION

After the success of cellular and Wi-Fi technologies in the last two decades, wireless communication has become a popular way of communication in people's day to day life [2]. Ad-Hoc networks have grown in a thick and fast way as a result of increased need of eliminating fixed infrastructure, geographical dependence and complexity of deployment for critical applications such as IoT, Industrial IoT (IIoT), military operations, disaster relief management, maritime communications, intelligent transportation systems, wild-life monitoring, health monitoring and many more.

Over the last few years, the problem of routing security has become a major concern for researchers. As required for the effective operations, routing protocol designed must be efficient and secure to ensure timely and reliable data transmission between vehicles [4].

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 [7]. 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,

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-6, 2019

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.

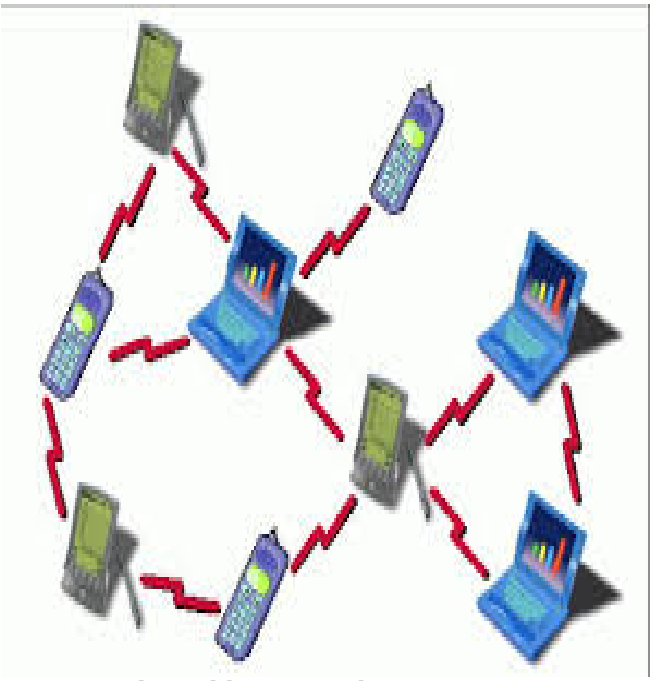

Fig 1: Wireless ad-hoc network.

Both safety applications and commercial applications are important for VANETs. Safety applications relate to human life, health, and well being, and commercial applications often benefit companies in the industry [1]. Thus, the development of safety and commercial applications can encourage the evolution of VANETs. For safety applications, the periodic broadcasting of beacons plays an important role because the status of neighbours such as their geographical positions, speeds, directions, and other important information are usually provided by the beacons of neighbours to discover each other in time. The accurate and efficient neighbor-hood discovery link layer services guarantee the safety of the road environment. For commercial applications, the effective transmission of various application data (such as data from so called 'infotainment') is desirable. For example, it is available for passengers to watch television shows or use the multi person video conferencing application in the vehicles.

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. In section II we discuss about the wireless communication introduction and wireless communication in vehicular ad-hoc network, In section III we discuss about the literature survey in the vehicular ad-hoc network, In section IV we discuss the about protocol layers or OSI model, finally in section V we conclude the about our paper.

II WIRELESS COMMUNICATION

The area of wireless communications will continue to grow for many reasons. People are becoming accustomed to immediate access to information wherever their locations, and technological improvements have made providing universal telecommunications access feasible. There currently is an expansion in the number of personal mobile radio networks that are the systems used by law enforcement groups, ambulance services, and on the floor of factories. The signals are meant to be relatively short-range and communication takes place on designated frequency ranges where they will not interfere with other applications such as wireless or mobile phones. In the near future there will be significant growth in wireless for the office, such as wireless local area networks and wireless private branch exchanges [9]. New developments in personal communications systems (PCS) include integrated phone/paging/email/data transmission. Currently handheld units are offered by the major wireless

industries with many of these features. These units range from cell phones with email capability, wireless pen tablets (low-end laptops without keyboards – interaction is via a pen), PDAs, and personal organizers.

Wireless communication is the transfer of information or power between two or more points that are not connected by an electrical conductor. The most common wireless technologies use radio waves. With radio waves distances can be short, such as a few meters for Bluetooth or as far as millions of kilometers for deep-space radio communications. It encompasses various types of fixed, mobile, and portable applications, including two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking [11].

III RELATED WORK

Hui Xia , San-shun Zhang et al. [1] In this paper they first study trust properties and construct a novel trust inference model, where two trust attributes named subjective trust and recommendation trust, are selected to quantify the trust level of a specific vehicle. The SCGM(1,1)-weighted Markov prediction algorithm based on fluctuation recognition is utilized to calculate the subjective trust accurately, meanwhile a new evaluation method of recommendation credibility based on the feedback mechanism is introduced for the calculation of recommendation trust. They subsequently exploit the advantages of mesh structure and design a light-weight trust-aware multicast routing protocol (i.e., LTMRP), which can establish secure and reliable communication paths by selecting trusted relay vehicles. Xiaojie Wang, Zhaolong Ning, et al. [2] Vehicular social networks (VSNs), viewed as the integration of traditional vehicular networks and social networks, are promising communication platforms based on the development of intelligent vehicles and deployment of intelligent transportation systems. Passengers can obtain information by searching over Internet or querying vehicles in proximity through intra-vehicle equipment. Hence, the performance of content dissemination in VSNs heavily relies on inter-vehicle communication and human behaviors. However, privacy preservation always conflicts with the usability of individual information in VSNs. article provides the unique characteristics of privacy-preserving requirements and solutions for content dissemination in VSNs. It focuses on: 1) a comprehensive overview of content dissemination in VSNs; 2) the privacy issues and potential attacks related to content dissemination; and 3) the corresponding solutions based on privacy consideration. First, the characteristics of VSNs, content dissemination and its solutions in VSNs are revealed. Second, the privacy issues for content dissemination in the current VSN architecture are analyzed and classified according to their features. Hui Xia, San-shun Zhang et al. [3] The Intelligent Transportation System (ITS) is an important application area of the Cyber-Physical System (CPS). To further promote effective communication between vehicles, vehicular ad hoc networks (VANETs) have been widely used in the ITS. However, the communication efficiency in VANETs is not only affected by the external environment but also more vulnerable to malicious attacks. In order to address the above-mentioned issues, they propose a novel trust-based multicast routing protocol (TMR) to defend against multiple attacks and improve the routing efficiency. In the proposed trust model, direct trust is calculated based on Bayesian theory and indirect trust is computed according to evaluation credibility and activity. The fuzzy logic theory is used to fuzzify the direct and indirect trust values, and then the total trust value of the node is obtained by defuzzification. Rutvij H. Jhaveri, Narendra M. Patel, et al. [4] In their previous work, they devised a novel trust based scheme for MANETs in IIoT in order to identify adversaries following different kinds of attack-patterns before they actually launch packet dropping attacks. The scheme intended to isolate the adversaries at an early stage in order to improve the quality-of-services. In this work, they attempt to identify the best choices of values of distinct parameters by carrying out sensitivity analysis of the scheme. The sensitivity analysis is carried out in different

network conditions by taking packet delivery ratio and normalized routing overhead as the performance metrics, and varying the values of distrust threshold, trust component's weight and trust update interval. 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. Hui Xia, Zhetao Li, Yuhui Zheng et al. [5] In this study they abstract a novel light-weight subjective trust inference framework, which is divided into trust assessment and trust prediction. The process of node trust assessment is based on node's historical behaviours. Then utilizing the obtained trust data sequence, they introduce the SCGM(1,1)-weighted Markov stochastic chain measure to predict node's trust for future decision making. Experimental results have been conducted to evaluate the effectiveness of the proposed trust model. As an important security application, based on the standard On-Demand Multicast Routing Protocol (ODMRP), they make four major improvements which take the issue of trust into consideration, and propose a novel trust-based routing protocol called the On-Demand Trust-Based Multicast Routing protocol (ODTMRP). And finally, convincing experimental results are presented using three routing evaluation metrics. Shuo Chen, Athirai A. Irissappane, et al. [6] This work proposes a POMDP-based approach to assist efficient decision-making for handling unforeseen events in VANETs. The POMDP model optimally queries information about uncertain events from neighboring vehicles while taking into account their malicious behavior. It better trades off the decision quality and the cost/delay incurred during information collection compared to the heuristic threshold based schemes. This work also considers the realistic setting where the observation function representing the behavior of neighbors needs to be learned and proposes a learning algorithm that can handle dynamic scenarios where malicious
Vehicles change their behavior from time to time. Experiments demonstrate that the proposed POMDP approach can make decisions faster without sacrificing quality. The experiments under dynamic scenario verify that the learning algorithm can learn the observation function efficiently while still handling behavior change effectively. Farhan Ahmad, Virginia N. L. Franqueira, Asma Adnane et al. [7] They 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. Their 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. Farhan Ahmad, Asma Adnaney, et al. [8] In this paper, they provided a comparative study of three TMs from each category, i.e., ETM, DTM and HTM. Further, they adopted a simulation-based approach where the efficiency of these TMs is evaluated against MITM attacks. Simulation results indicated that ETM outperformed other TMs due to the presence of role-based and experience-based trust techniques which ensured the dissemination of trusted information among vehicular entities. Further, the results also depicted that DTM and HTM are more prone to MITM attacks. This study can be used as a guideline by the researchers in order to design new TMs. They conclude that the future TMs should include role-based and experience-based trust management techniques to provide a trusted environment for message dissemination. As a future work, they will design an efficient TM which integrates these trust management techniques in order to achieve overall network security.

IV PROTOCOL LAYERS

The Open Systems Interconnection (OSI) model is a universal ISO standard, known as ISO protocol suite, which was introduced in 1970's by the

ISSN: 2581-3404 (Online)
International Journal of Innovative Research in Technology and Management (IJIRTM), Volume-3, Issue-6, 2019

International Organization for Standardization. Because of the different types of systems in large networks required to interoperate, the OSI model was created to facilitate the communication between two different systems by operating in a common framework. The OSI model consists of seven layers, the application, presentation, session, transport, network, data link and physical. We will study and analyze for this thesis the protocol architecture, considering the application, presentation and session layers as a whole, named application layer. The Internet protocol stack with the five layers is based on the TCP/IP model, which is the predominant model nowadays and was developed in the late 1960's by the Defense Advanced Research Projects Agency (DARPA).

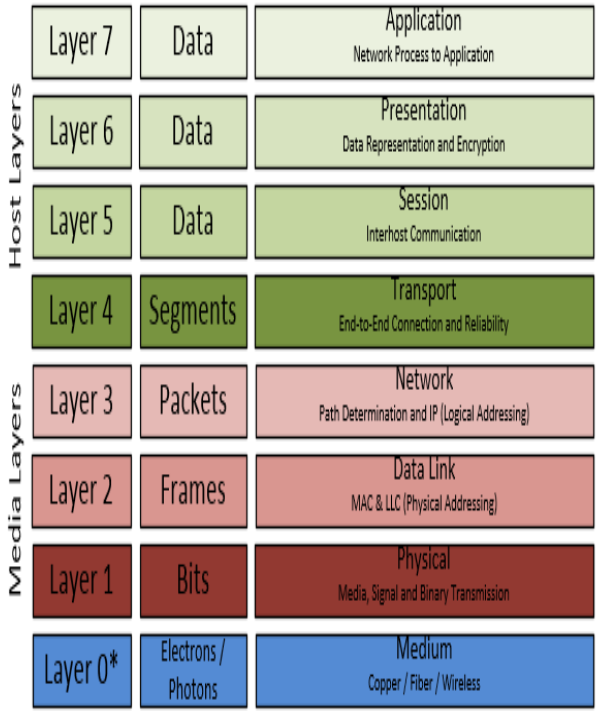

Fig 2: The Internet protocol stack.

In the above network protocol layering, each layer is required to establish communication between two hosts or nodes. Data from the application layer is forwarded to the next layer. Each layer adds a header and forwards the packet to the next layer until reaching the physical layer, where the packet is transmitted through the physical media.

V CONCLUSIONS

The term wireless communication was introduced in the 19th century and wireless communication technology has developed over the subsequent years. It is one of the most important mediums of transmission of information from one device to other devices; in the present day wireless communication system has become an essential part of various types of wireless communication devices that permits user to communicate even from remote operated areas. In this paper we present the literature survey for the wireless communication in the vehicular ad-hoc network.

REFERENCES:-

[1] Hui Xia , San-shun Zhang , Ye Li, Zhen-kuan Pan, Xin Peng, Xiu-zhen Cheng, "An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol 68, 2019, pp 7108-7120.

[2] Xiaojie Wang, Zhaolong Ning, Meng Chu Zhou, Xiping Hu, Lei Wang, Yan Zhang, Fei Richard Yu, Bin Hu, "Privacy-Preserving Content Dissemination for Vehicular Social Networks: Challenges and Solutions", IEEE Communications Surveys & Tutorials, 2018, pp 1-33.

[3] Hui Xia, San-shun Zhang, Ben-xia Li,1 Li Li, Xiang-guo Cheng, "Towards a Novel Trust-Based Multicast Routing for VANETs", Security and Communication Networks, 2018, pp 1-13.

[4] 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 2018, pp 20085-20103.

[5] Hui Xia, Zhetao Li, Yuhui Zheng, Anfeng Liu, Young-June Choi, Hiroo Sekiya, "A Novel Light-weight Subjective Trust Inference Framework in

MANETs", IEEE Transactions On Sustainable Computing, 2018, pp 1-14.

[6] Shuo Chen, Athirai A. Irissappane, Jie Zhang, "POMDP-Based Decision Making for Fast Event Handling in VANETs", The Thirty-Second AAAI Conference on Artificial Intelligence, 2018, pp 4646-4653.

[7] Farhan Ahmad, Virginia N. L. Franqueira, Asma Adnane, "TEAM: A Trust Evaluation and Management Framework in Context-Enabled Vehicular Ad-Hoc Networks", IEEE 2018, pp 28643-28661.

[8] Farhan Ahmad, Asma Adnaney, Fatih Kurugollu, Rasheed Hussain, "A Comparative Analysis of Trust Models for Safety Applications in IoT-enabled Vehicular Networks", IEEE 2017, pp 1-9.

[9] Nitha C Velayudhan, A.Anitha, Mukesh Madanan, Vince Paul, "Review On Avoiding Sybil Attack In Vanet While Operating In An Urban Environment", Journal of Theoretical and Applied Information Technology, 2019, pp 2267-2279.

[10] Zishan Liu, Zhenyu Liu, Lin Zhang, Xiaodong Lin, "MARP: A Distributed MAC Layer Attack Resistant Pseudonym Scheme for VANET", IEEE, 2018, pp 1-15.

[11] Ilhem Souissi, Nadia Ben Azzouna, Tahar Berradia, Lamjed Ben Said, "Fuzzy Logic based Model for Energy Consumption Trust Estimation in Electric Vehicular Networks", International Conference on Security and Cryptography, 2018, pp 221-233.

[12] Farhan Ahmad, Jordan Hall, Asma Adnane and Virginia N. L. Franqueira," Faith in Vehicles: A Set of Evaluation Criteria for Trust Management in Vehicular Ad-hoc Network", IEEE,2017, pp 44-52.

Chandni Ahirwal received her Bachelor`s degree in Electronics Comunication Engineering from TIT, Bhopal, M.P., in 2014. Currently she is pursuing Master of Technology Degree in Electronics & Comunication (Digital communication) from PCST, (RGPV), Bhopal, Madhya Pradesh India. Her research area include wireless communication.

Mr. **Jitendra Mishra** he is Associate Professor and Head of the Department of Electronics and communication in PCST, Bhopal (RGPV). His received Master of Technology and Bachelor's of engineering respectively in Digital communication from BUIT, Bhopal and from RGPV, Bhopal. He has more than 12 years of teaching experience and publish 50+ papers in International journals, conferences etc. His area of Interests is Antenna & Wave Propagation, Digital Signal Processing, Ad-hoc network, Wireless Communication, Vehicular Ad-hoc network, Image Processing etc.