IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-7, July 2019 E-ISSN: 2347-2693

Vanet Security and Privacy – An Overview

D.Kumar[1]* V.Sindhu[2]*

[1,2]ECE Department ,U.I.E.T, MDU, Rohtak, India

Corresponding Author: baalikumar786@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i7.105108 | Available online at: www.ijcseonline.org

Accepted: 15/Jul/2019, Published: 31/Jul/2019

***Abstract*--**Nearly 1.5 million people die from vehicles accidents per year and nearly 20 million are injured or physically disabled. we can be avoided 60 percent of accidents by using sufficient warnings system. For increasing safety in vehicles, we have Vehicular Ad hoc networks (VANETs) system. This System Designed to increase safety, driving efficiency and make the driving experience more reliable. VANETs connect vehicle into a huge mobile ad hoc network share data on a bigger scale. However, communicating in a free environment makes security and privacy issue an actual challenge, which may disrupt the VANETs system. Researchers have found a resolution to this problem. In this paper, I talked about the different techniques and security parameter which may reflect security and privacy in VANET system.

***Keywords*--** VANETs, Attacks, SECURITY AND PRIVACY REQUIREMENTS

I. INTRODUCTION

A **Vehicular Ad-Hoc network** is a type of Mobile Ad-hoc Networks, to provide vehicles communication among nearby vehicles and nearby fixed equipment i.e. onboard units and roadside equipment. The Communication of vehicles is three types-1) Inter-vehicle communication abbreviated as IVC i.e. vehicle to vehicle communication,2) Vehicle to roadside communication abbreviated as RVC i.e. communication between the roadside unit (RSU) and vehicles,3)Inter-roadside communication i.e. communication between the roadside unit and the base station. The potential of VANET has to provide safety and traffic management. Vehicles can notify other vehicles of unsafe road conditions, traffic jamming, or risk stops. Fig 1.shows the basic architecture of VANET.[7][8]

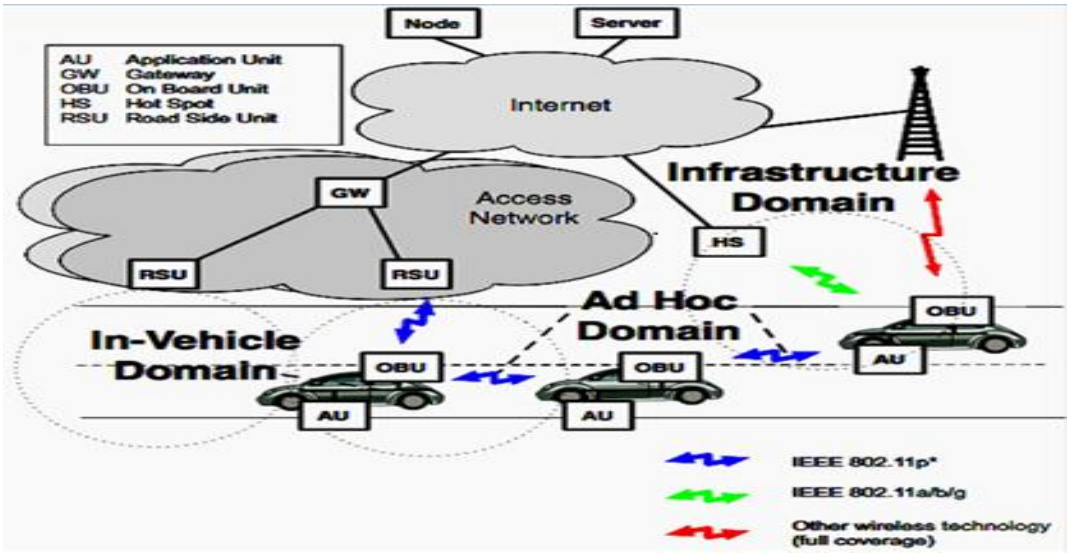

Fig.1 VANET Architecture

In a VANET, certain moving vehicles in an exceedingly little region constitutes a cell. It implies that the range of the wireless signal, i.e. transmitting zone from a moving vehicle is among a limited area (nearly 300 meters). A vehicle known as a node will do transmitting, receiving and routing (connecting) to different nodes while not facilitate of any

switch like Base Station (BTS) in mobile network or Access point (AP) in local area network or simply we can say direct communication between in vehicles and no need to access point[5] . Additionally, the moving vehicle in an exceedingly VANET will be connected to a different network like basic model network, internet, etc.

The range of spectrum for vehicle communication is specified by the federal communication commission. for IVC (Inter-Vehicle Communications) and RVC (Road to Vehicle Communications),the operating frequency is 700 MHz band[1,10]. This range is known as radio equipment of 700MHz band intelligent transport system. In 2017 this band enactment for IVC AND RVC. In ARIB STD-T109, IVC and RVC operate on a single channel by employing time division duplex which helps to avoid frame collisions between IVC and RVC. IEEE, 802.11p group describe the new physical layer and MAC (Medium access control) layer for inter-vehicular communication[1,10]. furthermore, in the IVC CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is used for communication between the vehicles which supports frequent inter-vehicle connectivity changes. but, this system suffers from a disadvantage of the increase in the frame collision probability because many vehicles may simultaneously start the IVC transmission procedure at the beginning of the IVC period.

II. SECURITY AND ATTACKS IN VANETS

Communication mainly depends on the exchange of the message. massage may be false which affect VANET systems. so security is a more crucial part of VANET system. Security concerns are more complex due to the false information of vehicles such as bogus information, false positioning of the vehicle, frequent topology changes, high mobility, and various applications.[3][4]

ATTACKS:
Attacks disrupted the communication system Attackers must be an insider (the member nodes who communicate other members) and outsider (intruder which aim to harms protocol).There are various types of attacks by attackers[3].

1. Denial of Service attack:
This attack happens when the attacker hacks or jams the main communication path and the network is no more workable for communication to each other nodes.

2. Message Suppression Attack:
An attacker selectively releasing packets from the network, these packets may hold significant information for the receiver, the attacker crushes these packets and can use them again in other time.

3. Fabrication Attack:
An attacker can make this attack by transmitting fake information into the network, the information could be invalid or the transmitter could pretend that it is somebody else This attack includes fabricate messages, warnings, certificates, identities.

4.Alteration Attack:
This attack happens when the attacker changes an existing data, it introduces delaying the transmission of the information, replaying more advanced transmission, or altering the actual entry of the data transmitted. For occurrence, an attacker can alter a message telling other vehicles that the current road is clear while the road is congested.

5.Timing Attack:
This attack arises when an attacker provides additional time(delay time) in the original message time slot. due to this original warning message sends to the nodes after mishaps occur.

6.Sybil Attack:
This attack appears when an attacker generates multiple numbers of pseudonymous massage which creates confusion between the nodes due to different source identity. this pseudonymous message acts like a traffic jam and forces them to take other routes.

7.Non-safety attacks:
It is part of the comfort of nodes and does not affect any safety applications. this attacks generally gives an effective traffic system. e.g car parking, a vehicle can adjust according to the parking slot.

III. SECURITY AND PRIVACY REQUIREMENTS SECURITY

After deployment of VANET, intelligent onboard applications keep a record of a large amount of vehicle movement data and individual information of the vehicle. Fraud or ill-usage of such information can lead to severe privacy and general security issues. There is a dire necessity to overcome these concerns before large-scale deployment of VANET.

Three basic security requirements that should be met in VANETs to deal with any threat, which is: authentication, integrity, availability and conditional privacy. These requirements are necessary so that every VANET system should observe[3,4].

Authentication
The basic and foremost requirement for vehicular network security is authentication. in VANET Authentication describes system confidential communication. Authentication is essential for verifying a claim of

authenticity. Particularly in VANET, authentication means confirming the identity of a vehicle and distinguishing genuine vehicles from unauthorized vehicles. It is important to make sure that the transmitted messages originate from real vehicles and not from non-existent nodes because transmission of malicious messages can lead to serious consequences like human injuries, traffic disruptions and in severe cases may even lead to death. Consequently, message authentication is important in VANET.

Integrity

Integrity stands the information of nodes are not altered by intruders. simply say data must be authentic means not modified.

Availability

Stands for the network must be available to the user or real nodes even it is attacked by an intruder.

Privacy in VANET SYSTEM

Unquestionably, a driver avails from the traffic-related messages that are automatically sent by other nearby vehicles. Despite, these messages include a sender's private information, such as the vehicle's integrity (plate license number), location, and direction. Simply, people are not interested to reveal this private information to third parties. Therefore, a reliable mechanism should stop an unapproved person from identifying the combination of real identity and other secret information. On the other hand, a committed authorization (e.g., police, sheriffs) has the right to reveal a vehicle's identity in case of illegal activity happening. Through, conditional privacy safety is necessary for VANET system.

IV. LITERATURE REVIEW

In this paper[2] discussed that Vehicular Ad Hoc Networks (VANET) has frequently earned the attention of today's research disciplines while current resolutions to obtain secure VANET, to defend the network from rival and attacks still not sufficient, trying to give a satisfying level, for the driver and manufacturer to attain the safety of life and infotainment. The necessity for a strong VANET network is fully dependent on their security and privacy features which will be presented in this paper. In this paper several kinds of security difficulties and challenges of VANET been examined and discussed; this also includes a set of clarifications conferred to solve these challenges and difficulties.

Group-based source authentication protocol using TESLA scheme. In this paper[13],Researchers suggested group based secure authentication using a public key method to verify the information authenticity in VANETs. Much VANETs application has real group property and VANET nodes follow an alike moving pattern. GSA makes use of group attributes as a dynamic group key to shield data transmission in intergroup communication, which is dynamically varying with the real-time environment and consistently modernizes among group members. TESLA protocol permits broadcast authentication without using digital impression all the time. The basic idea behind this protocol is the use of Hash chain(Generates many one-time key from single key or password)but there are numerous shortcomings to implement this method in VANETs. First, there is an initialization phase where the first element in the Hash chain has to be distributive to all the receiver. The set of the receiver should not vary during the usage of one hash chain. Second is the affirmation of messages is only probable once the next message is received, not adequate in delay-intolerant VANETs.

In this paper [4] authors discussed about Safety and security are enhancing the necessity for VANET application. As VANET use wireless technology it is exposed to many attacks. The several attacks in VANET are the Sybil attack DDOS attack, misbehaving and defective nodes, sinkhole attack, spoofing, traffic analysis attack, position attack, and an illusion attack. ways to prevent traffic analysis attack have been an ongoing area of research. Sybil attack is very dangerous in the geographical routing because a node can pretend to be in several positions at the same time. Sybil nodes may launch additional DOS(denial of service) attacks. Illusion attack is a new security threat to VANET application where produce erroneous sensor readings creating an illusion condition on VANET. The usual message authentication and integrity check used in the wireless network are low against the illusion attack. group of these attacks can be classified as active, passive and insider attacks. Existing detection tools for attacks in VANET have recommended various methods to identify, deal and provide a solution for each attack. Among these attacks collusion attack is a serious threat that assists an attacker to capture a car to have a clean gateway after a burglary or robbery.

This paper[3] discussed the distinct requirements for VANET networks which are completely dependent on their secrecy features and safety. The main purpose of this paper is to study the multiple attack detection technique and security issue in VANET. This paper provides the review of several attack detection technique such as Attacked Packet Detection Algorithm (APDA) which is related to detect the DOS attacks and cryptography and localization verifying technique which is used to solve the problem Sybil attack in VANET. The author further introduced the method of designing analysis tools in sequence to detect an attack in VANET. The proposed method is consists of parts: the Traffic Analyzer, the Fuzzification, the Fuzzy Inference Engine, the knowledge Base and Forensic Analyzer.

This research paper[13] reviewed the various security concerns such as confidentiality, authenticity, integrity, availability, and non-repudiation proposed to protect communication between vehicle to vehicle (V2V) and

vehicle to infrastructure (V2I). it reviewed and analyzed literature on the desirable security attacks from 13 researchers that address security and privacy concern in VANETs. This paper also gave the statistics on the relationship between security services versus the technique to face the possible attacks is listed. Five safety services including security attacks and techniques have been introduced.

V. CONCLUSION

In this paper we presented a concise overview on VANETs system. Also we have discussed various parameter and problems that occurs mostly in VANETs system. VANET to be widely accepted by society. If the VANETs security and privacy failures usually, pay only financial losses. VANET concern for improving the efficiency and safety of the vehicle. For example, the failure to identify a tempered vehicular message in time may prompt serious traffic mishaps, with loss of lives. This implies that every effort must be devoted to security and privacy concerns as a precondition for the wide adoption of VANETs.

REFERENCES

[1]. Zing Zhu, Sumit Roy, "MAC(Media Access Control) for DSRC (Dedicated Short Range Communication) in Intelligent Transport System", IEEE Commun. Mag., vol. 41, no. 12, pp. 60-67, Dec. 2003.

[2].G. Samara, Wafaa A.H. Al-Salihy, R. Sures" study of a security review of vehicular ad hoc networks (VANET)" National Advanced IPv6 Centre, Universitiy Sains Malaysia, 2010.

[3].K. B.Sahare and DR.L.G.Malik, " Review- Method for Detection of Attacks in VANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 2, February 2014.

[4]. M. Elsa Mathew and A.Raj Kumar p." threat examination and safety mechanisms in Vanet" international journal of advanced research in computer science and software engineering volume 3, issue 1, Jan 2013.

[5]. Ajmal, S., Rasheed, A., Qayyum, A., Hasan, A.: Classification of VANET MAC, Routing and approaches a detailed survey. J. UCS 20(4), 462–487 (2014).

[6]. Rasheed, A., Zia, H., Hashmi, F., Hadi, U., Naim, Warda, Ajmal, Sana: Fleet & convoy management using VANET. J. Comput. Netw. 1(1), 1–9 (2013).

[7]. Sajjad Akbar, M., Rasheed, A., Qayyum, A.: VANET architectures and protocol stacks: a survey. In: InternationalWorkshop on Communication Technologies for Vehicles, pp. 95–105. Springer, Berlin, Heidelberg (2011).

[8]. Liang, W., Li, Z., Zhang, H., Wang, S., Bie, Rongfang: Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. Int. J. Distrib. Sens. Netw. 2015, 17(2015).

[9]. Da Cunha, F.D., Boukerche, A., Villas, L., Carneiro Viana, A., Loureiro, Antonio AF.: Data communication in VANETs: a survey, challenges and applications. Ph.D. diss., INRIA Saclay; INRIA (2014).

[10]. Ajmal, Sana, Jabeen, Samra, Rasheed, Asim, Hasan, Aamir: An intelligent hybrid spread spectrum MAC for interference management in mobile ad hoc networks. Comput. Commun. 72, 116–129 (2015)

[11]. Marvy B. Mansour1, Cherif Salama2, Hoda K. Mohamed3 and Sherif A. Hammad4 1British University in Egypt, Cairo, Egypt 2,3Computer and Systems Engineering Department, Ain Shams University, Cairo, Egypt 4Avelabs, Cairo, Egypt – Munich, Germany.

[12].A. Yusri Dak, "A Literature Survey on Security Difficulties in VANETs", International Journal of Computer Theory And Engineering, Volume 4, No. 6, December 2012.

[13]. You Lu, Biao Zhou, Fei Jia, and M. Gerla, "Group-based Secure Source Authentication(GSA) Protocol for VANETs", IEEE Globecom 2010 Workshop on Heterogeneous, Multi-hop Wireless and Mobile Networks.

[14]. Road Safety Facts — Association for Safe International Road Travel.

