INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume2, Issue6)
Available online at: www.ijariit.com

Review of VANET Security on Trust Base

Diljot Kaur
Lovely Professional University
Diljot.sandhu22@gmail.com

Simarjit Singh Malhi
Lovely Professional University
Simarjit.15976@lpu.co.in

Abstract—In Trust based Networks; nodes are typically being controlled by realistic entities such as people. Trust based Network is aiming at enabling communication through highly heterogeneous networks by relying on dynamic nature of message transmission whenever there is arise in communication opportunities, such communication thus does not rely on a routing infrastructure and is peer-to-peer in nature. The delay-tolerant paradigm is akin to trust based networks, thus a suitable approach to address the lack of connectivity and the mobility. In this thesis we simulate attack and are monitoring the nodes by Particle swarm optimization, thus preventing the attack and which will lead to through put increase and overhead reduce.

Keywords—VANET, Security, DTN, Trust, ACO.

I. INTRODUCTION

Over the years, Vehicular Ad hoc Networks (VANETs) has emerged persuading the Mobile Ad-Hoc Networks (MANETs) to Vehicle-to-Vehicle and Vehicle-to-Roadside remote correspondence. In today's scenario transportation system plays a vital role. In the past decade a current transportation system which has been captivated much consideration from the aspects of both industry as well as academia. This has been expected from this new kind of introduced network to firmly provide support to distributed applications which are mobile in nature in case of vehicles [1].

Traffic safety, has been the main concern for many countries [4]. Many accidents are caused by in sufficient traffic information and by slow driver reaction to local visual and acoustic inputs. VANETs (Vehicular Ad-hoc Networks) overcome these problems by enhancing both the accuracy of traffic information and the delivery of alarms, thus provide help to avoid crashes. In VANET, cars commune through the help of wireless channel. They send packets straight forward to their neighbours inward radio range. Alternatively, intermediary cars route and forward packets to intended destinations. Communication is peer-to-peer, without centralized coordination. In VANETs, cars can exchange routine information such as current speeds, locations, directions, as well as emergency alarms like notifications of emergency braking, etc. With VANETs, cars can collect more accurate traffic information electronically with respect to drivers who are attaining information visually. Direct activation of commands (brakes, accelerator, steering wheel, etc.) by an alarm will ensure a car's prompt reaction without depending on the driver's alertness [9].

VANETs are becoming the most relevant wireless mobile technology. It's one of the capable perspectives to employ Intelligent Transportation Systems (ITS). VANETs are different from MANETs in terms of high node mobility, large scale networks, a geographically constrained topology that is highly dynamic, strict real time deadline, unreliable channel conditions, unavoidably slow deployment, and uneven connectivity between nodes, driver behavior and frequent network fragmentation. A VANET is a particular kind of Mobile Ad hoc network (MANET) that delivers messages in between a nearby motor vehicles and road side equipment. In this type of network, vehicles are considered to be the communication nodes that are considered to be the part of a self-manageable network without having any prior set of information about each other's presence in the entire network. There are two categories of nodes: On-Board Units (OBU) and Road Side Units (RSU). OBU provides the communication capabilities

among the vehicles, while RSUs are placed along the road and constitute the network infrastructure. RSUs work as a router between the vehicles. With the use of Dedicated Short Range Communication (DSRC) radios, OBUs can link the vehicle to RSUs. Therefore it is crucial that all the activities that are performed on VANET must be protected from malicious attacks. Various novel issues are connected with a VANET are because of special features of the network. To get start, the main distinctions in case of VANET and a MANET is that MANET typically has no infrastructure possible. Moreover, the greatest challenge is the mobile nature of vehicles in the network, speed of nodes is greater than the nodes in MANETs, leading to the path breaks. In addition, the two essential apprehensions for a VANET are security and privacy. Introduction of On board Global Positioning System (GPS) has brought the revolution in case of driving.

II. APPLICATIONS OF VANET SECURITY

To deploy VANETS, applications play an important role that is categorized on 2 classifications:

Safety Related Application: Users expands the security on the road and additionally classifieds in the subsequent method:

- Collision Avoidance: From some examination, 60% mishaps can be rid off if drivers get cautioning a large portion of a moment before crash. On the off chance that a driver gets a notice message on time, crash can be avoided**.**
- Cooperative Driving: If drivers can get indication for activity related notices like varying speed warning. These signs can participate in continuous and safe driving.
- Traffic Optimisation: Maximized with the use of transferring signals like jam, accidents etc. to the vehicles.

User Based Application: Supplies the customer infotainment. These are classified in the following ways:

- Peer to peer application**:** are functional to facilities like distributing songs, movies etc. between the motor vehicles in the system.
- Internet Connectivity: User required interrelating the web constantly (internet all the time).
- Other services: utilized in other user on the basis of application alike payment examine to gather the toll assessment, to position the petroleum station, eating place etc.

Vehicular Ad hoc Network is a division of MANET. Individual node meets with rest of the nodes specifically on multi hop. Vehicular Ad hoc Network delivers secure and non secure armed forces to the drivers. Vehicular Ad hoc Network composed small range radios installed in vehicles, Road Side Units and middle establishment which is account able intended for individuality registration and organization. However, difficult task for Vehicular Ad hoc Network to protect from the exploited behavior, safety structural design have to be cautiously intended particularly when it is all over the world employed. The safety of Vehicular Adhoc Network is most serious problems due to transferable among hubs. [12].

III. ATTACKERS ON VEHICULAR NETWORK

VANET requires security to employ the wireless environment and serves users with safety and non-safety approaches. Attacker produces distinct kinds of attack in vehicular environment. The aim of attacker is to establish issues for rest of users by modifying the message content in the network. Unintended users can be categorizing accordingly:

- Passive Attackers: These attackers listen to gather activity data which might be passed on to different attacker. As these attacker don't take an interest in the correspondence procedure of the system, so these attacker are called passive
- Active Attacker: Either produce packets composing wrong information or don't forward the data.
- Insider Attackers: Reliable customer of the system and have in depth information of association. When they have all data about the system then it's simple for them to dispatch attacks.
- Outsider Attackers: These type of attacks are done by the outside person who is not the part of the system.
- Malicious Attackers: They are actually not being benefited personally from the entire attack, so the main motive is to disrupt the functioning of the network or to harm others. They are known to be the dangerous one.

- Rational attacker: Their main concern is being benefited personally, and is mainly concerned about nature of target.
- Local attacker: This kind of attack is area specific in nature with a limited scope.

VANET technology represents positive benefits, alike a minimal amount of road mishappenings. Road users employ various applications for safety and efficiency, traffic management, warning, comfort, maintenance, music sharing and network gaming [8]. These applications involve the exchange of messages such as emergency message distribution, traffic incidents and road condition warnings that enhance traffic safety and driving efficiency, requires data sharing among hubs. Driver's behaviour impacts the message content, leads to topology change and security is in danger if message gets altered by unintended user [9].

IV. VANET SECURITY ARCHITECTURE

Security mechanisms in MANETs have been extensively studied; however, they are not suitable for VANETs due to the unique characteristics of VANETs, so they can't be directly applied to VANETs. Despite a broad range of challenges facing securing vehicular communication, the security issues must be addressed and solved for the successful deployment of VANETs. Since the drivers and the vehicles in VANETs rely on shared information to make decisions, they would be vulnerable to malicious and misbehaving nodes; so proper mechanisms need to be implemented for detecting and avoiding attacks from such malicious nodes. The security services of VANETs typically need to meet the following needs:

- Integrity: Integrity is to deal the accuracy, consistency, and the completeness of messages during transmission. In order to prevent attackers from altering or injecting messages, integrity of messages should be ensured. Also, a reliable time source for accurate time synchronization and a reliable positioning system for precise location sequence might be used to secure message against attacks alike replay-strike or position spoofing attack.
- Availability: In VANETs, time critical messages such as emergency traffic information must be handled at any given time. If one channel is not available due to failure or attack, there must be alternative means to maintain vehicular network availability all the time.
- Authentication: Every message exchanged must be authenticated to identify the sender of the message. Vehicles should react only to information or events generated by legitimate senders.
- Non-repudiation: This service is designed to identify misbehaving nodes or attackers and prevent them from denying messages transmitted by them. Any vehicle related information for communication, such as location, speed, and time, will be stored in a tamper-proof On-Board Unit. It also could be used by authorities for investigation to reproduce the scene of an accident with the same series and content of the messages communicated prior to accident.
- Real-time constraints: Vehicles move with high velocity. In some situations like time-sensitive communication, a real-time response is essential, so time constraints should be respected.
- Privacy: All driver information such as identity, location and speed, should be protected against unauthorized observers. Also, an observer should not be able to trace the routes of the vehicles.

Challenging issues in VANET

- Technical Challenges: The dealing of technical challenges is with the technical obstacles which can be determined prior to the operation of Vehicular Adhoc Network. Following are the few challenges:
- Network Management: Because of high mobility, the system topology and the channel circumstance transform quickly. Because of this, it is not possible to use structures such as tree because these design changes similar like the topology changes.
- Congestion and Collision Control: Challenge is generated by unbounded network size. Due to heavy traffic at the time of rush hours, there for system is very busy and an accident takes place in the systems.
- Environmental Impact: For communication VANET uses the electromagnetic waves. With the help of environment waves are exaggerated. It has been proved that in the deployment of the VANET, the main consideration is environmental impact.
- MAC Design: Vehicular Adhoc Network usually practices the communal medium to correspond consequently. MAC Design is the foremost problem.

- Security: Vehicular Adhoc Network delivers the road security uses which are considered to be life serious hence safety of the communication must be contented.

V. Social and Economical Challenges: It is a major problem to encourage a corporation to construct a system that delivers the traffic signal contravention due to customer may repel for example type of monitoring. So to encourage the VANET developer is a difficult task.

VI. LITERATURE REVIEW

Wang Suwan and He Yuan (2016) [1] "A Trust System for Detecting Selective Forwarding Attacks in VANETs," This paper, we address the problem of distinguishing specific sending assaults by building a trust framework. The proposed way to deal with keep up this framework for the most part incorporates (1) Mutual monitoring is used for finding the attacks between nodes by using the local and global information and (2) detect of attacker node based upon abnormal or bad driving patterns of malicious nodes. Since both in-band and out-band data is used, our approach is powerful in generally low-thickness street conditions and strong to different situations, for example, extraordinary rate of malignant event or diverse street's range. VANET is a natural high portability and take information sending as an essential instrument to share data among vehicles. Selective forwarding attack are the attack in which masquerade nodes acts as a normal nodes which drop data packets, damage the real or same form of data and damages the legitimacy of genuine VANETs applications. It is very difficult to obtain the selective forwarding attack because the attacker node always act as a normal node and always clash with each other whenever they want to change the integrity of data and damage to VANET system. The results of our simulations shows that our approach accomplishes a high fault tolerance with the help of by selecting most accurate nodes which is used for sending information, while in the meantime recognize attacker nodes with moderately high accuracy.

Chirayil Greeshma and Thomas Ashly (2016) [2] "A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement," Considers a few existing technologies such as CROWN, Vehicular Cloud and VANET-Cloud and a comparison on these is carried out. As the technology has to be used widely, there is a high need for a low cost VANET technology with high security and Quality of Service. To go for any further developments, a thorough analysis on the available technologies is essential to get a closer view on the current scenario. The result of this study can open doors for a better technology for future VANETs. It is very effectively used in VANET, a spontaneous creation of wireless system of vehicles for exchanging information between them, for improved traffic management and to ensure several users that are sufficiently up to date about the road and make safer and smarter decisions on road by using transport networks.

Qian Yi et. al. (2008) [3] "Design of Secure and Application-Oriented VANETs," Recommended safe and uses dispose system design structure for VANET and considered in cooperation safety needs of the interactions & necessities of possible Vehicular Ad hoc Network uses and facility. Different applications and private administrations are additionally allowed keeping in mind the end goal to bring down the cost and to empower VANET organization and appropriation. Security is one of the major issue that must be tended to before the deploy of VANETs can be effectively conveyed. Another critical issue is support of diverse applications and administrations in VANETs. Planned system composed of two prime apparatus: a control system of application-aware and a combined direction-finding method. Moreover the system design structure, they additional study an amount of main permission technologies that are important to a realistic Vehicular Adhoc Network. The research make available a instruction for the design of a more protected and practical VANET.

Lin Xiaodong et. al. (2008) [4] "Security in Vehicular Ad Hoc Networks," We reviewed the modern consistency development, that overspread the techniques of delivering safety favours & preserving driver isolation for Wireless Access in Vehicular Environments uses. They tackle two prime issues, official document repeal and provisional confidentiality protection, for building the values realistic. Moreover, a collection of unique safety strategy which is launched for gaining secure documentation repeal and restrictive privacy conservation, which are measured amongst the foremost demanding design reason in VANET. VANET promising way to deal with encouraging street security for drivers and travellers. One of the extreme objectives in the outline of such systems administration is to oppose different pernicious misuse and security attack.

Kaur Mandeep and Mahajan Manish (2015) [5] "A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs," This proposed model has been designed to detect and the DDoS strikes in the Vehicular Ad hoc Network clusters to prevent misshapen in the form of Vehicular Ad hoc Network node break down, accident. The DDoS strike anticipation algorithm mechanism as the actual time strike discovery and transparency information refine algorithm with respect to safe guard alongside the DoS and DDoS strike. The optional representation productivity has been gathered based on system weight, throughput, packet liberation ratio, etc. The investigational outputs have showed the efficiency of the considered representation in assessment with the existing models.

Kaur Mandeep et. al. (2016) [6] "Protection against DDOS Using Secure Code Propagation in the VANETs," Proposed model threats caused by DDoS attack with the use with the use of road side traffic management recommended a strong safety system to mitigate. The RTMU used several arithmetical calculations for traffic sample examines to detect the abnormality in data traffic among the cluster nodes. Also all of the VANET nodes communicate with each other through RTMU. The outputs have provide

efficiency of the recommend model to moderate the DDoS strike and make possible for horizontal transfer society. Vehicular Ad hoc Network used for mechanically determined vehicles in the forbidden surrounding. Although the human vehicles uses the Vehicular Ad hoc Network for further ability, the mechanically determined vehicles entirely rely leading the Vehicular Ad hoc Network. Any invasion in the Vehicular Ad hoc Network by hackers can reason prime traffic chaos. A famous technique called as prankster attack which is used by army-force to plot attacks to reason extra injure as possible by self-centered drivers to create their method obvious.

Harsch Charles et. al. (2007) [7] "Secure Position-Based Routing for VANETs," Delivers a strategy which safeguard geographic position-based routing, accepted as the sufficient one for VC. Furthermore, focused on strategy presently selected & appraised in the Car2Car Communication Consortium and incorporated safety strategy defending the position-based routing operationality and services which improves the systems strength. They recommend protection strategy, depending both on cryptographic essentials and prospect checks descriptive counter feit position addition. Our execution and introductory estimations demonstrate that the security overhead is low and the proposed plot deployable.

Amoozadeh Mani et. al. (2015) [8] "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving," Introduces a prime glance at the possessions of safety strikes on the statement channel and also sensor diversity of a linked car water course prepared attaining CACC. Their simulation output proves that an attack can reason important volatility in the CACC motor vehicle. Moreover, it has demonstrated how to calculate, alike degraded to ACC mode, might probably used to improved the safety and security of the associated motor vehicle streams. Alike classification depend greatly on board sensors alike cameras. Autonomous motor vehicle organize established extremely harsh provisions on the safety of the communiqué canal used by motor vehicle to replace in order as well as the manage reason that near complex driving works alike modify motor vehicle speed.

Kamani Jaydip and Parikh Dhaval (2015) [9] "A Review on Sybil Attack Detection Techniques," Briefly presents various Sybil attack detection mechanism in VANET. In Vehicular Communication, the security system against the attacker is very important. Sybil attacks considered a major safety hazard to ad hoc systems and sensor systems. It is an attack in which an original identity of the vehicle is corrupted or theft by an attacker to creates multiple fake identities. Detecting such type of attacker and the original vehicle is a challenging task in VANET.

Raya Maxim and Hubaux Jean (2007) [10] "Securing vehicular ad hoc networks," This paper concentrate on the safety of systems. They delivered a brief hazard examine and plan suitable safety structural design. Moreover, explain few chief design arrangements immobile to be complete, which in few cases which have than simple technical significance. They deliver a place of safety rules, and proved that they preserve isolation and observed the strength and efficiency.

Yan Gongjun (2008) [11] "Providing VANET security through active position detection," Vehicle position is a standout amongst the most important bits of data in a Vehicular Ad hoc Network (VANET). The fundamental commitment of this work is a novel way to deal with upgrading position security in VANETs. We attained limited safety by engaging by helping on-board radar to perceive adjoining motor vehicles & verify their disclosed integrates. Restricted safety is comprehensive & gets worldwide safety with the use of current position-based groups to generate a message system & with the use of active demanding system verifying distant location in sequence. The outcome is declared on the broadly conventional hypothesis that the huge greater part of motor vehicles is reliable and behaves correct. Widespread simulations verify the excellence of recommend outcome by calculating speedy negotiated motor vehicles can be identified under several circumstances.

Lim Kiho (2016) [12] "Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive-Based Architecture for Vehicular Cloud," In this paper VANETs permits to motor vehicles to outline a self-manageable system. VANETs are likely to be widely deployed in the future, given the interest shown by industry in self-driving cars and satisfying their customers various interests. Problems related to Mobile ad hoc Networks (MANETs) such as routing, security etc. have been extensively studied. Even though VANETs are special type of MANETs, solutions proposed for MANETs cannot be honestly applied to VANETs because all problems related to MANETs have been studied for small networks. Moreover, in MANETs, nodes can move randomly.

Rabieh Khaled (2015) [13] "Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs," In this paper, we discuss a cross-layer plan to empower the RSUs to distinguish such Sybil vehicles. Since Sybil vehicles don't exist in their asserted areas, our plan depends on checking the vehicles' areas. A test parcel is sent the vehicle's guaranteed area utilizing directional reception apparatus to recognize the nearness of a vehicle. On the off chance that the vehicle is at the normal area, it ought to have the capacity to get the test and send back a substantial reaction parcel. With a specific end goal to decrease the overhead and as opposed to sending challenge parcels to every one of the vehicles constantly, bundles are sent just when there is a doubt of Sybil assault. We likewise examine a few Sybil assault disturbing methods. The assessment comes about show that our plan can accomplish high recognition rate with low likelihood of false caution. Moreover, the plan requires. In Vehicular Ad Hoc Networks (VANETs), the roadside units (RSUs) need to know the quantity of vehicles in their region to be utilized as a part of activity administration. In any case, assailant may dispatch a Sybil assault by putting on a show to be numerous synchronous vehicles. This assault is extreme when a vehicle intrigues with others to utilize substantial qualifications to validate the Sybil

vehicles. In the event that RSUs can't distinguish such an assault, they will report wrong number of vehicles to the movement administration focus, which may bring about spreading incorrectly movement directions to vehicles.

Jain Kashma and Goyal Dinesh (2016) [14] "Design and Analysis of Secure VANET Framework preventing Black Hole and Gray Hole Attack," This paper scrutinized the effects of packet loss in the network due to Black Hole and Gray Hole attacks and also propositions a detection technique that competently detects both attacks in the network. In this research paper simulation is completed by using NS-2 simulator. In this research work the attack is performed and detected on AODV routing protocol. Furthermore, to determine the effects on attacks on network performance simulation is performed on different network scenarios. Vehicular Networks are considered as novel class of remote systems, likewise called as VANET (Vehicular specially appointed Networks). It is a key part of Intelligent Transport System (ITS). VANET innovation is distinguished for enhancing street security and transport effectiveness. In any case, because of late emerge in security issues in VANET; VANETs must have a protected route for correspondence which is very testing and imperative issue.

Rawat Ajay (2012) [15] "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS," This paper presents the wide spread research of available strikes & their available outcomes. (VANET) is a promising pattern in system. A current type of MANET, In VANET motor vehicles are the nodes with flexibility so don't have permanent communications & handle secure and non-safe uses in a wireless intermediate which makes it susceptible to various strikes. Safety is the main significant apprehension in VANET because of open access medium.

Engoulou Richard Gilles et. al. (2014) [16] "VANET security surveys," It provides a study of the safety problems & the limitations produced. Many Several classifiers of uses in VANETs are launched, also some safety necessities, pressure & convinced construction are recommended to resolve the safety issues. Lastly, worldwide safety construction for Vehicular Adhoc Network is recommended. The prime advantages of Vehicular Adhoc Network improved road security and vehicle security although defensive drivers isolation from strikes by adversary. Safety the most difficult problems in relation to Vehicular Adhoc Network while the information transferred circulated in open surroundings. This paper exhibits a study of the security issues and the difficulties they produce. The different classes of uses in VANETs are presented, and additionally some security prerequisites, dangers and certain designs are proposed to take care of the security issue.

Chim Tw et. al. (2011) [17] "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs," This paper recommended two safe and confidentiality improving connections strategy for Vehicular Ad hoc Networks to tackle messages and cluster communication for inter related-vehicle communication so that security and privacy can be provided to vehicles and also followed the prospects of leasing RSU toward assisting auto graph confirmation procedure. Existing arrangements either depend intensely on a sealed equipment gadget, or can't fulfil the security necessity and don't have a viable message confirmation plot. In this paper, we give a product based arrangement which makes utilization of just two shared privileged insights to fulfil the protection necessity (with security investigation) and gives lower message overhead and no less than 45% higher effective rate than past arrangements in the message check stage utilizing the sprout channel and the paired inquiry procedures (through recreation examine). We likewise give the primary gathering correspondence convention to permit vehicles to confirm and safely speak with others in a gathering of known vehicles.

Baniasadi Zohreh et. al. (2011) [18] "Modelling Composite Intrusion Detection Systems Using Fuzzy Description Logics," In this paper we propose another technique to help overseeing and directing security in vast systems. We utilize Fuzzy Description Logics (FDL) to show a composite Intrusion Detection framework (CIDS). We demonstrate that this half breed technique is more productive than fresh ones in complex situations. In this intrusion detection system is used if any type of unauthorized access is happened in the system.

Ghaleb Fuad A (2013) [19] "Security and Privacy Enhancement in VANETs using Mobility Pattern," It presented a sample dependent mis behaviour identification prospects in Vehicular Ad hoc Networks. Simulation outputs showed with the aim of the place Anonymous Message on the basis of prospects having capability to enhance safety & preserve confidentiality in Vehicular Adhoc Networks. This paper is introducing a versatility design based misconduct recognition approach in VANETs.

Raw Ram Shringar (2013) [20] "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET," Discussed about Vehicular Adhoc Networks & procedural and safety limitations, moreover described several main strikes and outcomes that which could be executed alongside these strikes. In this article, we have talked about the VANET and its specialized and security challenges. We have additionally talked about some real assaults furthermore, arrangements that can be executed against these assaults. We have thought about the arrangement utilizing diverse parameters. Ultimately we have examined the instruments that are utilized as a part of the arrangements.

Alheeti Khattab M. Ali (2015) [21] "An Intrusion Detection System Against Malicious Attacks on the Communication Network of Driverless Cars," This paper proposed two techniques that are anomaly based and mistreat detection to perceive the spiteful attack and also designed an ID scheme for Vehicular Ad hoc Networks with the use of Artificial Neural Networks for identifying Denial of Service (DOS) strikes. Using ns-2 simulator the outputs of this study are reviewed. The principle part of IDS is to identify the assault utilizing information produced from the system conduct such as a follow record. The IDSs utilize the

components extricated from the follow record as auditable information. In this paper, we propose oddity and abuse location to recognize the pernicious assault.

CONCLUSIONS

By utilizing the social attributes, the mobile nodes are building "Identity Trust" relationship. Meanwhile, the successors generate "Verified Feedback Packets" for positive behaviour being possessed by nodes and consequently the "Behaviour Trust" relationship is formed for slow-moving nodes. Simulation results shows that, by implementing this trust scheme, the delivery probability and trust reconstruction ratio can be effectively improved when there are large numbers of compromised nodes, and it means that this trust management scheme is efficient.

REFERENCES

[1] Wang Suwan and He Yuan (2016) "A Trust System for Detecting Selective Forwarding Attacks in VANETs", Springer International Journal, vol. XX, no. XX, pp. 377–386.

[2] Chirayil Greeshma and Thomas Ashly (2016) "A Study on Cost Effectiveness and Security of VANET Technologies for Future Enhancement", Procedia Technol., vol. 25, no. Raerest, pp. 356–363.

[3] Qian Yi et. al. (2008) "Design of Secure and Application-Oriented VANETs", IEEE, pp. 2794–2799.

[4] Lin Xiaodong et. al. (2008) "Security in Vehicular Ad Hoc Networks", IEEE Communications Magazine, pp. 88-95.

[5] Kaur Mandeep and Mahajan Manish (2015) "A Novel Security Approach for Data Flow and Data Pattern Analysis to Mitigate DDOS Attacks in VANETs", International Journal of Hybrid Information Technology, vol. 8, no. 8, pp. 113–122.

[6] Kaur Mandeep et. al. (2016) "Protection Against DDOS Using Secure Code Propagation In The VANETs", International Journal of Enginering Sciences, vol. 17, no. XX, pp. 573–577.

[7] Harsch Charles et. al. (2007), "Secure Position-Based Routing for VANETs", IEEE, pp. 26–30.

[8] Amoozadeh Mani et. al. (2015) "Security Vulnerabilities of Connected Vehicle Streams and Their Impact on Cooperative Driving", IEEE communication magazines, no. June, pp. 126–132.

[9] Kamani Jaydip and Parikh Dhaval (2015) "A Review on Sybil Attack Detection Techniques", Journal for Research, vol. 01, no. 01, pp. 27–31.

[10] Raya Maxim and Hubaux Jean (2007) "Securing vehicular ad hoc networks", Journal of computer Security, vol. 15, pp.39–68

[11] Yan Gongjun (2008) "Providing VANET security through active position detection", Computer communications, pp. 1–15.

[12] Lim Kiho (2016) "Secure and Authenticated Message Dissemination in Vehicular ad hoc Networks and an Incentive- Based Architecture for Vehicular Cloud", theses and Dissertations--Computer Science, paper 48.

[13] Rabieh Khaled (2015) "Cross-Layer Scheme for Detecting Large-scale Colluding Sybil Attack in VANETs", IEEE Communication and Information Systems Security Symposium, pp. 7298–7303.

[14] Jain Kashma and Goyal Dinesh (2016) "Design and Analysis of Secure VANET Framework preventing Black Hole and Gray Hole Attack", International Journal of Innovative Computer Science and Engineering, vol. 3, no. 4.

[15] Rawat Ajay (2012) "VANET: SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS", Journal of Information and Operatins Management, vol. 3, no. 1, p. 7762.

[16] Engoulou Richard Gilles et. al. (2014) "VANET security surveys", Comput. Communications, vol. 44, pp. 1–13.

[17] Chim Tw et. al. (2011) "SPECS: Secure and Privacy Enhancing Communications Schemes for VANETs", Scholars Hub, pp. 189–203.

[18] Baniasadi Zohreh et. al. (2011) "Modeling Composite Intrusion Detection Systems Using Fuzzy Description Logics", International Symposium on Computer Networks and Distributed System, pp. 1–6.

[19] Ghaleb Fuad A (2013) "Security and Privacy Enhancement in VANETs using Mobility Pattern", IEEE ICUFN, vol. XX.

[20] Raw Ram Shringar (2013) "SECURITY CHALLENGES, ISSUES AND THEIR SOLUTIONS FOR VANET", International Journal of Network Security and its applications, vol. 5, no. 5, pp. 95–105.

[21] Alheeti Khattab M. Ali (2015) "An Intrusion Detection System against Malicious Attacks on the Communication Network of Driverless Cars", Consumer communications and Networking Conference, pp. 916–921.

