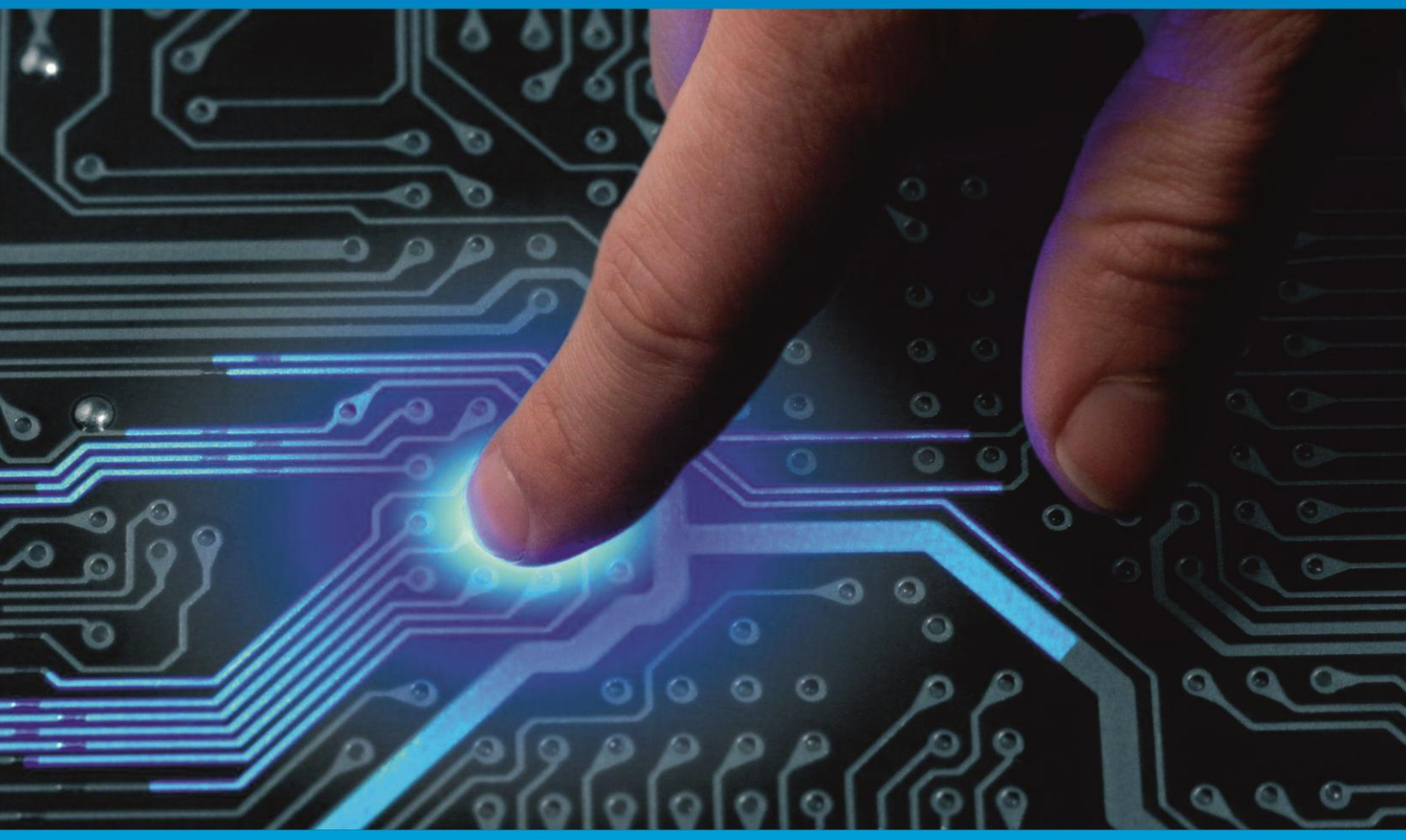
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 1, January 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

Review on Security Attacks and Possible Solution in Wireless Sensor Networks

Poonam[1], Prof. Nitesh Kumar[2]

M.Tech Scholar, Dept. of ECE., Sagar Institute of Research Technology & Science, Bhopal, India[1]

Assistant Professor, Dept. of ECE., Sagar Institute of Research Technology & Science, Bhopal, India[2]

ABSTRACT: Wireless Sensor Networks (WSN) is also known as Mobile Ad Hoc Networks, which is using for improvements of network traffic system. Since the movements of nodes are restricted by networks, traffic regulations can deploy fixed network at critical locations. We focus our study on the different kind of attacks and its behavior or impact in safety system and how many challenges; we have to accept for high security. In this paper we classify different attacks based on different layers like MAC layer, network, transport, application and multi layer and different challenges which included authentication, availability Privacy, anonymity etc.

KEYWORDS: WSN, DOS, DDOS, MAC, Privacy.

I. INTRODUCTION

Wireless sensor network (WSN) is a significant component of intelligent transportation system, which facilitates vehicles to share sensitive information and corporate with others. However, due to its unique characteristics, such as openness, dynamic topology and high mobility, WSN suffers from various attacks. [1] Safety of human lives in the road is the major concern nowadays, because every year thousands of peoples died in road accidents over the world. Wireless sensor network (WSN) is special kind of network that aims to reduce death rate and improves traffic safety system. Wireless sensor network (WSN), the promising technique, is getting attention for managing the traffic efficiently and making the road safe. The topographies and its vast applications varying from road safety, to the traffic management, payment service to infotainment. WSN are characterized as a self-organized, distributed, highly mobile, dynamic topology, unconstrained power, computational and storage networks. The communication in WSN is performed in open-access environment which demands the security issues must be deal with utter importance. Security requirements includes authentication, availability, message confidentiality, message integrity, data availability, access control, privacy, message non-repudiation and real time guarantees of message delivery.[2]

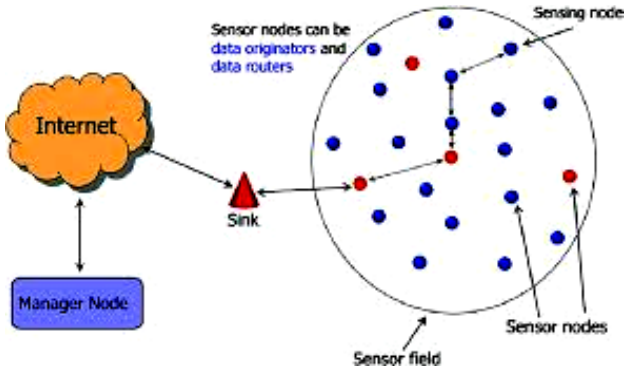


Figure 1: Architecture of WSN

Wireless sensor network (WSN) is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected. In WSN, moving vehicles as nodes can send and receive safety messages to each other on the road to ensure safety of human life [1]. WSN turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As vehicles fall out of the signal range and drop out of the network, other vehicles can join in, connecting vehicles to one another so that a mobile Internet is created.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

The primary goal of WSN is to provide road safety measures where information about vehicle's current speed, location coordinates are passed with or without the deployment of Infrastructure. Apart from safety measures, WSN also provides value added services like email, audio/video sharing etc.

Dedicated Short Range Communication (DSRC) is the frequency band that is used as a DSRC delivers safety and non safety messages in entire network by using its safety and non safety channels. Non safety applications are related to comfort of the passengers and to improve the traffic system. Parking availability and toll collection services are examples of these applications. Security is an important issue especially in this kind of network where one altered message can creates problem for the users in many ways. Attackers create problem directly and indirectly by launching different kind of attacks.

II. RELATED WORK

O. R. Ahutu et al., Nodes in wireless sensor networks (WSN) are resource and energy-constrained because they are generally batteries powered and therefore have limited computational capability. Due to the less secure environment in WSN, some malicious nodes at one point can tunnel packets to another location to damage the network in terms of packets dropping and eavesdropping and this is a so-called wormhole attack. Many of the current protocols solve the wormhole attack problem in isolation from the node energy consumption. However, some other proposed solutions consider reducing the energy consumption to detect such attacks but still it is needed to probe better performance. [1]

A. K. Goyal et al., proposed a secure and efficient WSN infrastructure, an extensive overview of characteristics, challenges, security attacks and requirements must be dealt with. The prime objective of this paper is to provide a classification of security requirements, security characteristics and challenges. [2]

D. P. Choudhari et al., analyzing the packet delivery ratio (PDR) for the network under Eavesdropping and DDoS attacks and after removal of these attacks the packet delivery ratio (PDR) is increased for the network. The Packet Delivery Ratio i.e. PDR is the number of packets received and the packets generated as recorded in trace file. So we define Packet Delivery Ratio as the total numbers of packets received at the destination to the total number of packets send form the source. [3]

R. Kolandaisamy, et al., proposed a novel scheme attack detection using vehicle mode analysis in Exploratory Based Ant Colony Approach (EBACA) for WSN is proposed. The underlying assumption is that a mode analysis of vehicles specifies reliability and unreliability of messages they drive. With mode, all evident information on a vehicle is submitted to provide past, current and even prospect activities and its transmission activities. [4]

B. Luo, et al., proposes a blockchain enabled trust-based location privacy protection scheme in WSN. Specifically, by analyzing the different requirements of the request vehicle and the cooperative vehicle during the process of constructing the anonymous cloaking region, as well as combining the characteristics of these two roles, we devise the trust management method based on Dirichlet distribution, such that both the requester and the cooperator will only cooperate with the vehicles they trust.[5]

Y. Zeng et al., present a perturbation-based causative attack which targets at the supply chain of DL classifiers in the WSN. We first train a classifier using WSN simulated data which meets the standard accuracy for identifying malicious traffic in the WSN. Then, we elaborate on the effectiveness of our presented attack scheme on this pre-trained classifier. We also explore some feasible approaches to ease the outcome brought by our attack. Experimental results show that the scheme can cause the target DL model a 10.52% drop in accuracy. [6]

W. Li et al., proposes a Sybil nodes detection method based on RSSI sequence and vehicle driving matrix - RSDM. RSDM evaluates the difference between the RSSI sequence and the driving matrix by dynamic distance matching to detect Sybil nodes. Moreover, RSDM does not rely on WSN infrastructure, neighbor nodes or specific hardware. The experimental results show that RSDM performs well with a higher detection rate and a lower error rate. [7]

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

Y. Gao et al., proposed detection system consists of two main components: real-time network traffic collection module and network traffic detection module. To build our proposed system, we use Spark to speed up data processing and use HDFS to store massive suspicious attacks. In the network collection module, micro-batch data processing model is used to improve the real-time performance of traffic feature collection. In the traffic detection module, the classification algorithm based on Random Forest (RF) is adopted. In order to evaluate the accuracy of detection, the algorithm was evaluated and compared in the datasets, containing NSL-KDD and UNSW-NB15. The experimental results show that the proposed detection algorithm reached the accuracy rate of 99.95% and 98.75%, and the false alarm rate (FAR) of 0.05% and 1.08%, respectively, in two datasets. [8]

J. R. et al., primarily focuses on detecting the malicious node that pretends to be a legitimate vehicle throughout the session hijacking attack in WSN and also discusses on the throughput, delay at end points, total counts of packet generated, exchanged and dropped using the Network Simulator-2 (NS2) tool and appropriate inference provided. [9]

M. Poongodi et al., proposed reCAPTCHA controller mechanism prevents the automated attacks similarly like botnet zombies. The reCAPTCHA controller is used to check and prohibit most of the automated DDoS attacks. For implementing this technique, the information theory based metric is used to analyze the deviation in users request in terms of entropy. Frequency and entropy are the metrics used to measure the vulnerability of the attack. [10]

S. Kumar et al., proposed a packet detection algorithm for the prevention of DoS attacks is proposed. This algorithm will be able to detect the multiple malicious nodes in the network which are sending irrelevant packets to jam the network and that will eventually stop the network to send the safety messages. The proposed algorithm was simulated in NS-2 and the quantitative values of packet delivery ratio, packet loss ratio, network throughput proves that the proposed algorithm enhance the security of the network by detecting the DoS attack well in time. [11]

A. M. Alrehan et al., focus on studying the main attacks along with DDoS attack on WSN system as well as exploring potential solutions with a focus on machine learning based solutions to detect such attacks in this field. [12]

R. N. Nabwene et al., Trust establishment in WSN helps deal with insider attacks, although most of the existing solutions assume the attacker will always show a stable dishonest behavior over time, which is not the case with intelligent insider attackers, they exhibit intelligent behaviors to avoid detection. In this Paper we review existing solutions used in misbehavior detection with primary concern on intelligent attacks like the adaptive detection threshold, evaluation of trust among vehicles for independent time periods and draw conclusions, as well as give suggestions on future research to mitigate intelligent attacks. [13]

T. Zaidi et al., Due to frequent change in topological structure, it is very difficult to make a WSN secure. In this research article, it is being observed that many security challenges are there where research have to step-up forward for making WSN more secure. A critical analysis is discussed broadly with respect to WSN components, security issues and challenges, attacks and its solutions. [14]

S. Hamdan et al., shows an improved algorithm will be proposed, taking advantage the footprint and privacy-preserving detection of abuses of pseudonyms (P2DAP) methods. The hybrid detection scheme will be implemented using the ns2 simulator. P2DAP acting better than footprint when the number of vehicles increases. In the other hand, the footprint algorithm acting better when the speed of vehicles increases. A new hybrid algorithm will be performed that depends on the encrypted, authentication and on the trajectory of the vehicle. The scenarios will be generated using SUMO and MOVE tools. [15]

A. M. R. Tolba et al., a trust-based distributed authentication (TDA) method that relies on a global trust server and vehicle behavior for avoiding collision attacks is proposed. This method ensures both inter-vehicular and intra-vehicular communication security in the network. In addition, a channel state routing protocol (CSRP) is proposed to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

improve the communication reliability among the vehicles. Reliable vehicles are identified according to the on-board unit (OBU) energy and the channel state of the vehicle to deliver seamless communication. [16]

III. WSN CHARACTERSTICS

In addition to the similarities to ad hoc networks, WSN possess unique network characteristics that distinguish it from other kinds of ad hoc networks and influence research in this area. Few important characteristics of WSN are as follows:

(i)High Mobility
(ii)Rapidly changing network topology
(iii)Unbounded network size
(iv)Frequent exchange of information
(v)Wireless Communication
(vi)Time Critical
(vii) Sufficient Energy
(viii)Better Physical Protection

A. WSN APPLICATIONS

Major applications of WSN include providing safety information, traffic management, toll services, location based services and infotainment

B. WSN ATTACKS

WSN suffer from various attacks; these attacks are discussed in the following subsections:

Greedy drivers: selfish drivers trying to maximize their gain by making believe a congested path to their destinations, and consequently suppress traffic by attacking the routing mechanisms.

Snoops: drivers attempting to profile drivers and extract their identifying information. Malicious Snoops can even track vehicle locations and determine the identities of drivers by corresponding them to the house or work sites.

Pranksters: drivers trying to disable applications or prevent information from reaching others vehicles. Such attacks are denoted by Denial of service attacks (DoS).

Malicious attackers: drivers deliberately attempting to make harm via the available applications within the network. Several attacks focus on damaging exchanged data between vehicles such as message fabrication, suppression or alteration. Sybil attack (Masquerade) [5]) belongs also to this category.

Industrial insiders: if vehicle manufacturers are responsible for securing communications within WSN, employees can reveal confidential data to malicious entities.

Jamming : The jammer deliberately generates interfering transmissions that prevent communication within their reception range. In the WSN scenario, an attacker can relatively easily partition the network, without compromising cryptographic mechanisms and with limited transmission power.

• Node Impersonation Attack

Each vehicle has a unique identifier in WSN and it is used to verify the message whenever an accident happens by sending wrong messages to other vehicles [4, 9, and 10]. Fig explains this scenario in which vehicle A involves in the

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

accident at location Z. When police identify the driver as it is associated with driver's identity, attacker changes his/her identity and simply refuses it.

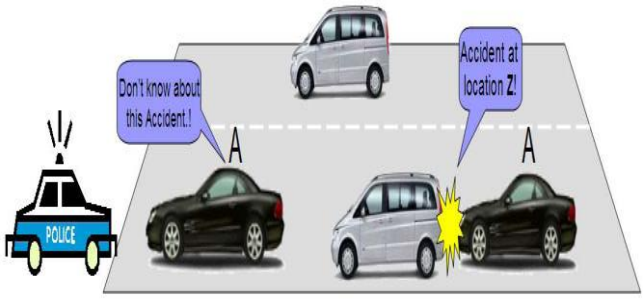


Figure 2: Node Impersonation Attack

• Sybil Attack

Sybil attack [10] so belongs to the first class. In Sybil attack, the attacker sends multiple messages to other vehicles and each message contains different fabricated source identity (ID). It provides illusion to other vehicle by sending some wrong messages like traffic jam message [3, 4]. Figure 3 explains Sybil attack in which the attacker creates multiple vehicles on the road with same identity. The objective is to enforce other vehicles on the road to leave the road for the benefits of the attacker.

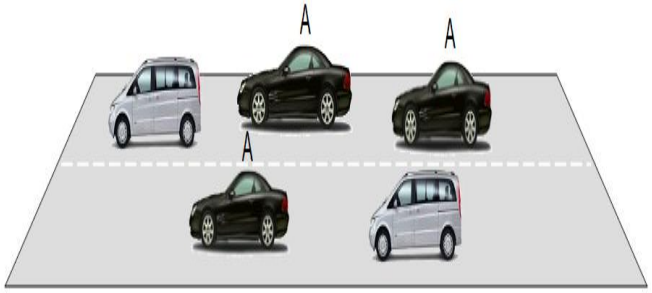


Figure 3: Sybil Attack

• Routing attack

Routing attacks re the attacks which exploits the vulnerability of network layer routing protocols. In this type of attack the attacker either drops the packet or disturbs the routing process of the network. Following are the most common routing attacks in the WSN:

a) Black Hole attack:

In this type of attack, the attacker firstly attracts the nodes to transmit the packet through itself. It can be done by continuous sending the malicious route reply with fresh route and low hop count. After attracting the node, when the packet is forwarded through this node, it silently drops the packet.

b) Worm Hole attack:

In this attack, an adversary receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. This tunnel between two adversaries are called wormhole. It can be established through a single long-range wireless link or a wired link between the two adversaries. Hence it is simple for the adversary to make the tunneled packet arrive sooner than other packets transmitted over a normal multi-hop route.

c) Gray Hole attack:

This is the extension of black hole attack. In this type of attack the malicious node behaves like the black node attack but it drops the packet selectively. This selection can be of two types:

i) A malicious node can drop the packet of UDP whereas the TCP packet will be forwarded.

ii) The malicious node can drop the packet on the basis of probabilistic distribution.

• Session hijacking

Most authentication process is done at the start of the session. Hence it is easy to hijack the session after connection establishment. In this attack attackers take control of session between nodes.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

Repudiation: The main threat in repudiation is denial or attempt to denial by a node involved in communication. This is different from the impersonate attack. In this attack two or more entity has common identity hence it is easy to get indistinguishable and hence they can be repudiated.

• Denial of Service

DoS attacks are most prominent attack in this category. In this attack attacker prevents the legitimate user to use the service from the victim node. DoS attacks can be carried out in many ways.

a) Jamming: In this technique the attacker senses the physical channel and gets the information about the frequency at which the receiver receives the signal. Then he transmits the signal on the channel so that channel is jam.

b) SYN Flooding: In this mechanism large no of SYN request is sent to the victim node, spoofing the sender address. The victim node send back the SYN-ACK to the spoofed address but victim node does not get any ACK packet in return. This result too half opens connection to handle by a victim node's buffer. As a consequence the legitimate request is discarded.

c) Distributed DoS attack: This is another form Dos attack. In this attack, multiple attackers attack the victim node and prevents legitimate user from accessing the service.

IV. CONCLUSION

In this paper various aspect of WSN like its architecture, application, attacks and challenges have been discussed; furthermore various characteristics of WSN have been listed which distinguished it from other networks like MANET. This paper includes various attacks in WSN have been classified depending on the different layers. It has been observed that the classification helps to deal with different types of attack in WSN. We have been discussed security challenge and security requirements. We have found after survey that attacks in multilayer like denial of services (DOS) and DDOS are very harmful for security system as well as authentication and Privacy are big challenges. In future we analyze vehicular network using hybrid prevention method.

REFERENCES

[1]. O. R. Ahutu and H. El-Ocla, "Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 63270-63282, 2020, doi: 10.1109/ACCESS.2020.2983438.

[2]. A. K. Goyal, A. Kumar Tripathi and G. Agarwal, "Security Attacks, Requirements and Authentication Schemes in VANET," *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, GHAZIABAD, India, 2019, pp. 1-5.

[3]. D. P. Choudhari and S. S. Dorle, "Maximization of packet delivery ratio for DADCQ protocol after removal of Eavesdropping and DDoS attacks in VANET," *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1-8.

[4]. R. Kolandaisamy, R. M. Noor, M. R. Zaba, I. Ahmedy and I. Kolandaisamy, "Markov Chain Based Ant Colony Approach for Mitigating DDoS Attacks Using Integrated Vehicle Mode Analysis in VANET," *2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP)*, Chennai, India, 2019, pp. 1-5.

[5]. B. Luo, X. Li, J. Weng, J. Guo and J. Ma, "Blockchain Enabled Trust-based Location Privacy Protection Scheme in VANET," in *IEEE Transactions on Vehicular Technology*.

[6]. Y. Zeng, M. Qiu, J. Niu, Y. Long, J. Xiong and M. Liu, "V-PSC: A Perturbation-Based Causative Attack Against DL Classifiers' Supply Chain in VANET," *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, New York, NY, USA, 2019, pp. 86-91.

[7]. W. Li and D. Zhang, "RSSI Sequence and Vehicle Driving Matrix Based Sybil Nodes Detection in VANET," *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, Chongqing, China, 2019, pp. 763-767.

[8]. Y. Gao, H. Wu, B. Song, Y. Jin, X. Luo and X. Zeng, "A Distributed Network Intrusion Detection System for Distributed Denial of Service Attacks in Vehicular Ad Hoc Network," in *IEEE Access*, vol. 7, pp. 154560-154571, 2019.

[9]. J. R. and N. S. Bhuvaneswari, "Malicious node detection in WSN Session Hijacking Attack," *2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT)*, Coimbatore, India, 2019, pp. 1-6.

[10]. M. Poongodi, V. Vijayakumar, F. Al-Turjman, M. Hamdi and M. Ma, "Intrusion Prevention System for DDoS Attack on WSN With reCAPTCHA Controller Using Information Based Metrics," in *IEEE Access*, vol. 7, pp. 158481-158491, 2019.

[11]. S. Kumar and K. S. Mann, "Prevention of DoS Attacks by Detection of Multiple Malicious Nodes in VANETs," *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, London, United Kingdom, 2019, pp. 89-94.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 1, January 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0901014 |

[12]. A. M. Alrehan and F. A. Alhaidari, "Machine Learning Techniques to Detect DDoS Attacks on WSN System: A Survey," *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)*, Riyadh, Saudi Arabia, 2019, pp. 1-6.

[13]. R. N. Nabwene, "Review on Intelligent Internal Attacks Detection in VANET," *2018 4th Annual International Conference on Network and Information Systems for Computers (ICNISC)*, Wuhan, China, 2018, pp. 1-6.

[14]. T. Zaidi and Syed.Faisal, "An Overview: Various Attacks in VANET," *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, Greater Noida, India, 2018, pp. 1-6.

[15]. S. Hamdan, A. Hudaib and A. Awajan, "Hybrid Algorithm to Detect the Sybil Attacks in VANET," *2018 Fifth International Symposium on Innovation in Information and Communication Technology (ISIICT)*, Amman, 2018, pp. 1-6.

[16]. A. M. R. Tolba, "Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs," in *IEEE Access*, vol. 6, pp. 62747-62755, 2018.

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details