A Survey on Security Attacks and Possible Solution in Wireless Sensor Networks

[1]Kolli Gnana Deepika, [2]Prof. Anoop Singh, [3]Dr. Varsha Namdeo
[1]Research Scholar, [2]Assistant Professor, [3]Associate Professor & HOD
[1&2&3]Department of Computer Science Engineering,
[1&2&3]RKDF Institute of Science & Technology, SRK University, Bhopal, India

Abstract : Wireless Sensor Networks (WSN) is also called Mobile Ad Hoc Networks, which is utilizing for enhancements of organization traffic framework. Since the developments of hubs are limited by networks, traffic guidelines can send fixed organization at basic areas. We center our examination on the diverse sort of attacks and its conduct or effect in wellbeing framework and what number difficulties; we need to acknowledge for high security. In this paper we study various attacks dependent on various layers like MAC layer, organization, transport, application and multi-facet and various difficulties which included confirmation, accessibility Protection, anonymity etc.

IndexTerms **- WSN, DOS, DDOS, MAC, Privacy.**

I. INTRODUCTION

Wireless sensor network (WSN) is a huge segment of smart transportation framework, which encourages vehicles to impart touchy data and corporate to other people. However, because of its one of kind qualities, like receptiveness, dynamic geography and high portability, WSN experiences different attacks. [1] Security of living souls in the road is the significant concern nowadays, in light of the fact that consistently thousands of people groups kicked the bucket in road mishaps over the world. Wireless sensor network (WSN) is exceptional sort of organization that plans to lessen demise rate and improves traffic security framework. Wireless sensor network (WSN), the promising strategy, is standing out enough to be noticed for dealing with the traffic productively and making the road safe. The geographies and its immense applications changing from road wellbeing, to the traffic the executives, installment administration to infotainment. WSN are portrayed as a self-coordinated, disseminated, exceptionally mobile, unique geography, unconstrained force, computational and capacity networks. The correspondence in WSN is acted in open-access climate which requests the security issues should be manage utter significance. Security necessities incorporates validation, accessibility, message classification, message respectability, information accessibility, access control, protection, message non-renouncement and continuous assurances of message delivery.[2]

Wireless sensor network (WSN) is important for Mobile Ad Hoc Networks (MANET), this implies that each hub can move uninhibitedly inside the organization inclusion and stay associated. In WSN, moving vehicles as hubs can send and get wellbeing messages to one another on the road to guarantee security of human existence [1]. WSN transforms each taking part vehicle into a wireless switch or hub, permitting vehicles roughly 100 to 300 meters of one another to associate and, thus, make an organization with a wide reach. As vehicles drop out of the sign reach and exit the organization, different vehicles can participate, associating vehicles to each other so a mobile Web is made.

The essential objective of WSN is to give road wellbeing estimates where data about vehicle's present speed, area facilitates are passed with or without the organization of Framework. Aside from security measures, WSN additionally offers some incentive added administrations like email, sound/video sharing and so forth.

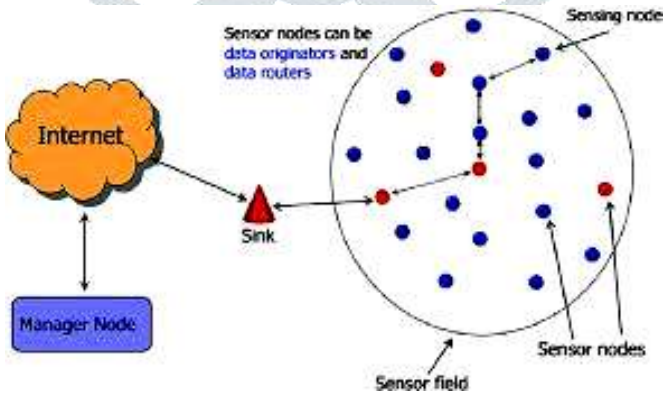

Figure 1: Architecture of WSN

Dedicated short range communication (DSRC) is the recurrence band that is utilized as a DSRC conveys security and non wellbeing messages in whole organization by utilizing its security and non wellbeing channels. Non wellbeing applications are identified with solace of the travelers and to improve the traffic framework. Stopping accessibility and cost assortment administrations are instances of these applications. Security is a significant issue particularly in this sort of organization where one modified message can makes issue for the clients from multiple points of view. Attackers make issue straightforwardly and in a roundabout way by dispatching diverse sort of attacks.

II. LITERATURE SURVEY

O. R. Ahutu et al., Hubs in wireless sensor networks (WSN) are asset and energy-compelled on the grounds that they are for the most part batteries controlled and subsequently have restricted computational capacity. Because of the less secure climate in WSN, some pernicious hubs at one point can burrow bundles to another area to harm the organization as far as parcels dropping and snoopping and this is an alleged wormhole attack. A considerable lot of the current conventions take care of the wormhole attack issue in separation from the hub energy utilization. However, some other proposed arrangements consider diminishing the energy utilization to recognize such attacks yet it is expected to test better execution. [1]

A. K. Goyal et al., proposed a protected and productive WSN foundation, a broad outline of attributes, challenges, security attacks and prerequisites should be managed. The great goal of this paper is to give an order of safety necessities, security qualities and difficulties. [2]

D. P. Choudhari et al., breaking down the parcel conveyance proportion (PDR) for the organization under Snoopping and DDoS attacks and after evacuation of these attacks the bundle conveyance proportion (PDR) is expanded for the organization. The Bundle Conveyance Proportion for example PDR is the quantity of bundles got and the parcels produced as recorded in follow document. So we characterize Parcel Conveyance Proportion as the all out quantities of bundles got at the objective to the absolute number of parcels send structure the source. [3]

R. Kolandaisamy, et al., proposed a novel plan attack identification utilizing vehicle mode examination in Exploratory Based Insect Province Approach (EBACA) for WSN is proposed. The basic supposition that will be that a mode examination of vehicles determines dependability and inconsistency of messages they drive. With mode, all apparent data on a vehicle is submitted to give past, current and even possibility exercises and its transmission exercises. [4]

B. Luo, et al., proposes a blockchain empowered trust-based area security insurance conspire in WSN. In particular, by examining the various prerequisites of the solicitation vehicle and the helpful vehicle during the way toward developing the unknown shrouding area, just as consolidating the qualities of these two jobs, we devise the trust the board method dependent on Dirichlet circulation, to such an extent that both the requester and the cooperator will just help out the vehicles they trust.[5]

Y. Zeng et al., present an irritation based causative attack which focuses at the production network of DL classifiers in the WSN. We first train a classifier utilizing WSN mimicked information which fulfills the guideline precision for recognizing vindictive traffic in the WSN. At that point, we expand on the viability of our introduced attack conspire on this pre-prepared classifier. We additionally investigate some plausible ways to deal with facilitate the result brought by our attack. Trial results show that the plan can cause the objective DL model a 10.52% drop in precision. [6]

W. Li et al., proposes a Sybil hubs identification method dependent on RSSI arrangement and vehicle driving network - RSDM. RSDM assesses the contrast between the RSSI arrangement and the driving network by powerful distance coordinating to identify Sybil hubs. Additionally, RSDM doesn't depend on WSN framework, neighbor hubs or explicit equipment. The trial results show that RSDM performs well with a higher location rate and a lower blunder rate. [7]

Y. Gao et al., proposed identification framework comprises of two principle parts: continuous organization traffic assortment module and organization traffic location module. To construct our proposed framework, we go through Flash to speed information preparing and use HDFS to store gigantic dubious attacks. In the organization assortment module, miniature group information handling model is utilized to improve the constant exhibition of traffic highlight assortment. In the rush hour gridlock identification module, the order calculation dependent on Arbitrary Timberland (RF) is adopted. [8]

J. R. et al., fundamentally centers around identifying the malevolent hub that claims to be an authentic vehicle throughout the meeting commandeering attack in WSN and furthermore talks about on the throughput, delay at end focuses, complete checks of parcel produced, traded and dropped utilizing the Organization Test system 2 (NS2) apparatus and proper deduction gave. [9]

M. Poongodi et al., proposed reCAPTCHA regulator system forestalls the mechanized attacks comparatively like botnet zombies. The reCAPTCHA regulator is utilized to check and deny the greater part of the computerized DDoS attacks. For executing this procedure, the data hypothesis based measurement is utilized to break down the deviation in clients demand as far as entropy. Recurrence and entropy are the measurements used to gauge the weakness of the attack. [10]

S. Kumar et al., proposed a bundle recognition calculation for the avoidance of DoS attacks is proposed. This calculation will actually want to recognize the different noxious hubs in the organization which are sending unimportant bundles to stick the organization and that will in the long run stop the organization to send the security messages. The proposed calculation was reenacted in NS-2 and the quantitative estimations of bundle conveyance proportion, parcel misfortune proportion, network throughput demonstrates that the proposed calculation improve the security of the organization by recognizing the DoS attack well on schedule. [11]

A. M. Alrehan et al., center around considering the fundamental attacks alongside DDoS attack on WSN framework just as investigating possible arrangements with an emphasis on machine learning based answers for identify such attacks in this field. [12]

R. N. Nabwene et al., Trust foundation in WSN assists manage insider attacks, although the vast majority of the current arrangements accept the attacker will consistently show a stable dishonest conduct after some time, which isn't the situation with keen insider attackers, they display astute practices to keep away from discovery. In this Paper we survey existing arrangements utilized in mischief recognition with essential worry on smart attacks like the adaptive identification threshold, assessment of trust

among vehicles for autonomous time spans and make determinations, just as give ideas on future exploration to relieve shrewd attacks. [13]

T. Zaidi et al., Because of successive change in topological design, it is hard to make a WSN secure. In this examination article, it is being seen that numerous security challenges are there where exploration need to venture up forward for making WSN safer. A basic investigation is talked about broadly regarding WSN segments, security issues and difficulties, attacks and its answers. [14]

S. Hamdan et al., shows an improved calculation will be proposed, exploiting the impression and protection safeguarding location of maltreatments of nom de plumes methods. The half and half location plan will be carried out utilizing the ns2 test system. P2DAP acting better compared to impression when the quantity of vehicles increments. In the other hand, the impression calculation acting better when the speed of vehicles increments. Another cross breed calculation will be played out that relies upon the scrambled, validation and on the direction of the vehicle. The situations will be created utilizing SUMO and MOVE apparatuses. [15]

A. M. R. Tolba et al., a trust-based appropriated verification (TDA) method that depends on a worldwide trust worker and vehicle conduct for staying away from crash attacks is proposed. This method guarantees both between vehicular and intra-vehicular correspondence security in the organization. In addition, a channel state steering convention (CSRP) is proposed to improve the correspondence dependability among the vehicles. Dependable vehicles are distinguished by the on-board unit (OBU) energy and the channel condition of the vehicle to convey consistent correspondence. [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:

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.

• 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 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.

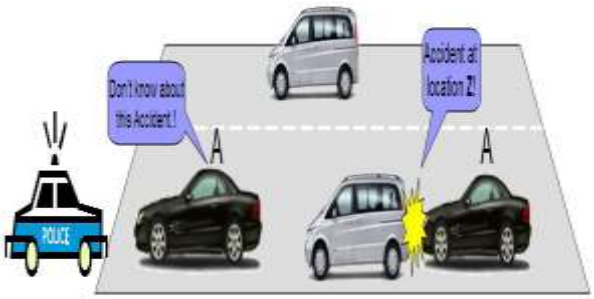

Figure 2: Node Impersonation Attack

• 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.

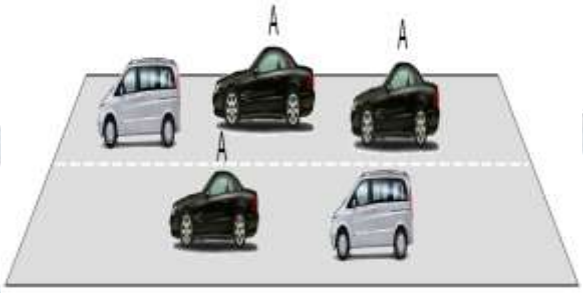

Figure 3: Sybil Attack

• 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.

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 different part of WSN like its design, application, attacks and difficulties have been examined; besides different qualities of WSN have been recorded which recognized it from different networks like MANET. This paper remembers different attacks for WSN have been ordered relying upon the various layers. It has been seen that the arrangement assists with managing various kinds of attack in WSN. We have been talked about security challenge and security necessities. 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.
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.