A Review On Different Attacks And Detection Approaches In Wireless System

Pardeep Kaur,
M.tech (ECE), Student
Punjabi University,
Punjab, India.
pairikaur@gmail.com

Dr. Harjinder Singgh
M.tech (ECE), Assistant Professor,
Punjabi University,
Punjab, India.
hrjindr@gmail.com

***Abstract*—the advancements in the current communication technology gives a rise to the wireless sensor network (WSN) based communication. The WSN can be categorized in various types like Vehicular Ad hoc network (VANETs), Mobile Ad hoc Networks (MANETs) and Flying Ad hoc Networks (FANETs). Out of these types of WSNs, the VANETs and MANETs are highly in demand. This study presents a review to the concept that how the communication and data transmission is performed in sensor network. Along with this, the major focus of this study is to analyze the various security threats and solutions to the data plane in network. This study has also presents a review to the work that had been done in past in order to resolve the data security issues in sensor networks.**

Keywords—Wireless Sensor Network, network security, routing, attacks, Sybil attack, black hole attack, worm hole attack.

I. INTRODUCTION

A Wireless Sensor Network (WSN) consists of a high number of autonomous sensor nodes and one or a few gateway nodes. Since the sensor nodes in the network have tiny size, therefore, these are also known as motes. These motes collect environmental information such as temperature, pressure, humidity, light conditions, movement and natural disasters using attached sensors [1]. This information travels wirelessly from a mote through the network until it reaches a gateway. During the forwarding, different routes might be taken depending on the availability of the sensor nodes routing tables [2]. The gateway node is normally connected to a computer from a different network in order to gather all the data sent from the WSN. These Wireless Sensor Networks (WSNs) are ad-hoc networks, where each sensor node participates in routing by forwarding information to other sensor nodes using the nearest neighboring communication. Without the use of a pre-defined infrastructure until the gateway is reached [3]. These gateways might be bridged with other gateways either to combine networks such as the Internet, or to extend the data transmission to a location that sensor nodes cannot reach [4].

II. SECURITY ISSUES IN WSN

Following are some of the security issues that can exist in WSN.

- The wireless networks are more prone to link attacks such as passive link attacks like eavesdropping and active link attacks like active interfering. Whereas in case of wired networks, the network is prevented from attacks by using firewalls and gateways but in case of wireless network the attacks can enter to the network from all directions and can aim at any node [5]. These attacks can reveal of confidential information. This can violates the rules of security hence it is mandatory that each and every node of the network should be capable to beat these kind of adversaries whether directly or indirectly.
- The sensor nodes in the network that are autonomous in nature are more prone to the attacks and unintended user's access. Therefore, the hacker or intruder can attack the nodes either from inside or from outside of the network. Since it is quite easy for the intruders to target such nodes and it is also hard to locate such attacks in the network [6].
- Any kind of security approach with the placement of the nodes is not approved to be sufficient enough in order to prevent the network from any kind of malicious activity. If the user of the network, wants the high availability of the network, a dispersed network without central entity must be employed. The central server in the network sometimes can become a strong reason behind the attacks in the network [7].

From above statements it is observed that even various types of security mechanisms are not capable to remove all types of vulnerabilities from the network. Various generalized security steps had been taken towards the direction of solution to various vulnerabilities such as cryptography etc [8]. From above points it is concluded that nodes should not trust on any other node immediately. Hence trust model can help the nodes to detect whether a node is trustworthy or not, weather a node is capable to take part is the process of routing or not.

III. ATTACKS IN DATA PLANE

In case of WSN, the network attacks can be categorized in two different categories as Active attacks and Passive attacks. In

active attack the certified or authorized node performs the data tempering whereas in passive attack the unauthorized node gains the access over the data without interrupting the networking operations [9]. Another form of classification of attacks divides the attacks in two categories as internal attack and external attack. The internal attack refers to the form of attack where the attacker node related to the network whereas in external attack the attacker node is from outside the network. Internal attacks are considered to be more rigorous as compare to the external attacks because in internal attack the victim nodes have all the access to the confidential information [10]. Various security issues in form of attacks such as worm hole attacks, grey hole attack, Denial of Service attacks etc had been studied in past [11]. The data over the WSNs can get infected if any of the following attack occurs in the network. There attacks are categorized in 4 parts as follows:

a) Black hole Attack:

A black hole attack [12] provides a shortest path of a destination node having a packet that a malicious node sends erroneous routing information and wishes to interrupt the packet, and in a destination, for example AODV, a malicious node argues that it can send a fake route response (RREP) to the source node and provide the shortest route and new route to the destination node. In this attack the malicious hub uses the techniques for routing protocol to recommend itself as a shortest path to other hubs.

b) Grey Hole Attack

Gray Hole Attack is a kind of active attack that guides to the destruction of data packets. It is sometimes called a black hole attack. In the Gray Hole attack nasty or malicious node is acting as normal node and drops the message or packets which is passing through them, hence hiding the important information to forward to the next node or destiny node [13].

c) Wormhole Attack

Wormhole attack is also known as tunnel attack. The wormhole attack is considered as the most serious attack in the network. In wormhole attack, the conspiracy nodes develop a tunnel from source node to destination node to transmit the data and to generate the smallest route. This is done by making it attractive to other nodes in the network. In wormhole attack, the data packets are dropped on the way by shorting the systematic flow of the data packets. The malicious node in a tunnel is capable enough to receive messages on a low latency in a specific portion of the network and replay these messages to the other part of the network [14].

d) Sinkhole Attack

Sink hole attack is considered as the most dangerous attack in WSN. The major focus in sink hole attack is that the attacker node attracts all the data traffic towards it by providing a shortest and attractive path for data transmission.

e) Denial of Service Attack

As per Wood and Stankovic, the denial of service attack is an event to reduce the network's capability in order to perform its functionality. Denial of service attacks has a specific role in WSN in which it is not feasible to handle the computing overhead in order to apply the typical attack defensive strategies of traditional computing. The jamming of the nodes is considered as a standard attack on the network.

f) The Sybil Attack

The Sybil Attack also referred as "malicious device illegitimately" operates multiple identities. Basically, it can be said as an attack that is competent to supervise the data duplication mechanism of distributed data storage system in point-to-point communication network.

g) Tampering

Tampering is a type of physical attack that exists in wireless networking. In this form of attack, the intruder gets access to the data via generating the fake sensor nodes. After having access to the data, the intruder can tamper the confidential data. Here in this attack, the tampering refers to the process to perform alterations in the data that travels in the network, to perform modification in the structure of the network in order to have a control to the network by the third party.

h) Other Attacks against Privacy

WSN technology promises a vast increase in automatic data collection capabilities through efficient deployment of tiny sensor devices. While these technologies offer great benefits to users, they also exhibit significant potential for abuse. Particularly relevant concerns are privacy problems, since sensor networks provide increased data collection capabilities [14]. The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from WSN could probably be collected through direct site surveillance. Rather, sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain surveillance. They can gather information in a low-risk, anonymous manner. Some of the more common attacks [15] against sensor privacy are:

- Monitor and Eavesdropping. This is the most obvious attack to privacy. By listening to the data, the adversary could easily discover the communication contents.
- Traffic Analysis typically combines with monitoring and eavesdropping. An increase in the number of transmitted packets between certain nodes could signal that a specific sensor has registered activity. Through the analysis on the traffic, some sensors with special roles or activities can be effectively identified [16].
- Camouflage. Adversaries can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can masquerade as a normal node to attract the packets, then misroute the packets.

- Exhaustion: In this the network resources are exhausted due to the frequent re-transmission of the data packets.
- Unfairness: This attack is a type of weak Denial of Service attack. In this attack, the focus of the invader is to degrade the overall performance of the network instead of accessing the complete data on the network.
- Spoofing: in this attack, the attacker directly attacks the routing information in the network. Since the routing information is quite large and confidential [17].

IV. RELATED WORK

Noor Alsaedia, 2015, **[1]** In civilian as well as military domains the wireless sensor networks were a rising technique utilized in several applications. Generally, in wireless as well as hostile conditions these networks were arranged. It was susceptible to several sorts of security attacks, of which sybil attacks were some of the most harmful. Therefore, it was required to resolve the issues associated to sensor node restraints as well as the necessitation for high WSN security. An Energy Trust System was projected in this work for wireless sensor networks in order to efficiently investigate Sybil attacks. On the basis of the identity as well as position verification the multi-level detection was employed in this. After that, on the basis of energy of every sensor node a trust paradigm was utilized. In order to decrease communication overhead as well as to save energy the data aggregation was also used. By applying theoretical as well as simulation-based mechanisms the performance of the projected mechanism was examined in case of protection as well as resource utilization. The simulation results had demonstrated that the projected ETS was efficient as well as robust in investigating Sybil attacks in case of the true as well as false positive rates. The projected mechanism attained more than 70% detection at the initial level by virtue of the application of multi-level detection that effectively enhanced to 100% detection at the secondary stage. Moreover, this mechanism decreased communication overhead, memory overhead and energy utilization through removing the exchange of feedback as well as suggested messages with sensor nodes.

Amol Vasudevaa, 2018, [2] In this paper the author had offered an overview of the most emerging mechanisms presented however to defend three modules of ad hoc networks that were Wireless sensor networks, Wireless Mesh networks and Mobile Ad-hoc Networks from the Sybil attack. By applying a random key pre-distribution, time difference of arrival, passive ad hoc Sybil identity detection, energy trust-based system, central authority, radio resource testing, neighborhood data, passive ad hoc Sybil identity with group detection and received signal strength indicator the mechanisms involved symmetric cryptography. Particularly, the author had examined several methods in order to mitigate the Sybil attack, together among its merits as well as demerits.

Mian Ahmad Janab, 2018, [3] In this work the author had projected a Sybil attack detection mechanism for a cluster-based hierarchical network generally employed to monitor forest wildfire. A two-tier detection mechanism was projected in this work. First of all, through high-energy nodes the Sybil nodes as well its forged identities were detected. Therefore, if one or more than one identities of a Sybil node sneak through the detection procedure, it was finally investigated by the couple of base stations. After the detection of Sybil attack an optimal percentage of cluster heads were selected as well as each one was updated through utilizing nomination packets. Every nomination packet consists of the identity of a selected cluster head as well as an end user's particular query for data collection in a cluster. To an end consumer necessitation these queries were user-centric, on-demand and adaptive. In one or more than one clusters the undetected identities of Sybil nodes were existed. The major concern was to send high false-negative alerts to an end user in order to divert attention to the geographical areas that were minimally vulnerable to a wildfire. The simulation results had demonstrated that the projected mechanism had offered enhanced lifespan of the network because of effective sleep-awake scheduling, low false-negative rate and higher detection rate.

Panagiotis Sarigiannidisa, 2015, [5] The major concern of this work was to defend against the Sybil attack. Through disrupting several networking protocols the Sybil attacks can merely deteriorate the system performance as well as compromise the security. A rule-based anomaly detection mechanism known as RADS was projected in this work that monitors as well as investigates the Sybil attacks in large-scale wireless sensor networks. At its center, the proposed expert framework depends on a ultra-wideband (UWB) ranging-based detection calculation that works in a disseminated way having no participation or data sharing between in sensor nodes so as to present the anomaly recognition assignments. At the time of the performance of RADS in exposing Sybil attacks was more assessed both mathematically and numerically, the possibility of the projected mechanism was verified analytically. The attained results had illustrated that high detection accuracy was attained by the RADS as well as low false alarm rate appointing it a promising ADS candidate for this group of wireless network.

Mojtaba Jamshidia, 2017, [6] Against WSNs the Sybil attack was a famous attack where a malicious node had tried to promulgate several identities. The routing protocols an several other functions like voting, resource allocation, data aggregation, misbehavior detection and so forth were affected negatively by the Sybil attack. In mobile WSNs a light weight, dynamic paradigm was projected in order to investigate Sybil nodes in this work. The projected paradigm had utilized Watchdog Nodes initially to label (*bit label*) mobile nodes on the basis of their movement behaviors, as well as after that investigated Sybil nodes consistent with the labels, throughout detection phase. The Sybil nodes had similar *bit label* as every Sybil node belong to a malicious node and move collectively. In the detection phase in order to detect the Sybil nodes this fact was utilized. In case of true detection as well as false detection rates the simulation results were compared among traditional paradigms. The simulation results were obtained by using JSIM simulator that demonstrated the projected paradigm was capable to identify more than 94% of Sybil nodes as false detection rate was 0%.

Meenakshi Tripathi, 2013, [7] The organization of Wireless Sensor Networks (WSN) in unattended condition had prompted different security dangers. This paper had offered an outline of LEACH, the most famous clustered routing protocol of WSN and how LEACH can be imperiled by Black hole and Gray Hole attacker. "High energy threshold" idea was utilized to simulate these attacks on NS-2. The execution of WSN under attack was completely examined, through utilizing it on different system parameters among different node densities. It was seen that the impact of the Black Hole attack was more on the system execution when contrasted with the Gray Hole attack.

Parmar Amisha, 2016, [8] Remarkable attributes like restricted bandwidth, constrained battery power and dynamic topology made Wireless sensor network (WSN) susceptible against numerous sorts of attacks. In this way interest for research of security in WSN had been expanding since most recent quite a long while. Framework less and self-administering nature of WSN was challenging problem in case of security. Wormhole attack was one of the serious attacks in wireless sensor attack. In this work, the systems managing wormhole attack in WSN were studied and a technique was proposed for discovery and anticipation of wormhole attack. Ad hoc on interest Multipath Distance Vector routing protocol was fused into these techniques which depend on Round Trip Time method and different qualities of wormhole attack. When contrasted with other arrangement appeared in literature, proposed method looks exceptionally encouraging. NS2 simulator was utilized to present the entire simulation.

David Airehroura Jairo, 2018, [9] In order to launch destructive and devastating attacks against an IoT network an attacker could exploit the routing mechanism of RPL. The Rank as well as Sybil attacks were prominent among these IoT attacks. In this work a time-based trust-aware RPL routing protocol was projected and executed in order to secure IoT systems from routing attacks. SecTrust-RPL had utilized a trust-based mechanism to identify and isolate attacks while upgrading system execution. The execution of SecTrust-RPL was contrasted and the standard RPL protocol. SecTrust-RPL protocol illustrated its better execution over the standard RPL protocol in the recognition and confinement of Rank and Sybil attacks. The adequacy and strength of SecTrust-RPL was shown through broad simulation analysis and testbed tests. In light of SecTrust-RPL, a proof-of-concept the feasibility of utilizing trust as an efficient security mechanism for mitigating attacks in IoT networks had shown as proof.

Samir Athmani, 2017, [10] In WSNs securing the network communication presented one of the most significant challenges. In classical wireless sensor networks contrarily to heterogeneous ones the key distribution issue had been broadly discussed. In the network through introducing high resource capability sensor nodes The Heterogeneous Wireless sensor networks had optimized the system ability and opened new security chances. For heterogeneous wireless sensor network an effective dynamic authentication and key Management mechanism was projected in this work. The major concept was to offer a single light weight protocol for authentication as well as key establishment throughout enhancing the security level. In order to produce dynamic keys and does not require any safe channel and sharing stage which enhances the security, energy effectiveness and lessens the memory utilization on the basis of which the key distribution paradigm was occurred. The simulation results had verified the presentations of our method comparative to the various traditional security protocols.

V. CONCLUSION AND FUTURE SCOPE

The data in sensor networks travels through the nodes in a wireless manner. Most of the sensor networks, did not follow a fixed infrastructure for the network, due to dynamic infrastructure, the sensor networks are considered to be more prone to the security attacks. This study has analyzed the work of various authors that has been done to improve the security of the data in the sensor networks. On the basis of the related work, it can be concluded that more amendments could be done in future by using the advance techniques.

REFERENCES

[1]. Noor Alsaedia, Fazirulhisyam Hashima, A. Salia, Fakhrul Z. Rokhani, "Detecting Sybil Attacks in Clustered Wireless Sensor Networks Based on Energy Trust System (ETS)", Elsevier, vol 110, pp 75-825, 2015

[2]. Amol Vasudevaa, Manu Soodb, "Survey on sybil attack defense mechanisms in wireless ad hoc networks", Elsevier, vol 120, pp 78-118, 2018

[3]. Mian Ahmad Janab, Priyadarsi Nandaa, Xiang jian, Hea Ren PingLiu, "A Sybil attack detection scheme for a forest wildfire monitoring application", Elsevier, vol 80, pp 613-626, 2018

[4]. Noor Al saedi, Fazir ul hisyam, Hashim A. Sali, Fakhrul Z. Rokhani, "Detecting sybil attacks in clustered wireless sensor networks based on energy trust system (ETS)", Elsevier, vol 110, pp 75-82, 2017

[5]. Panagiotis Sarigiannidisa, Eirini Karapistolib, Anastasios A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information", Elsevier, vol 42, issue 21, pp 7560-7572, 2015

[6]. Mojtaba Jamshidia, Ehsan Zangenehb, Mehdi Esnaasharic, Mohammad Reza Meybodid, "A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks", Elsevier, vol 64, pp 220-232, 2017

[7]. Meenakshi Tripathi, M.S. Gaur V. Laxmi, "Comparing the Impact of Black Hole and Gray Hole Attack on LEACH in WSN", Elsevier, vol 19, pp 1101-1107, 2013.

[8]. Parmar Amisha, V. B. Vaghela, "Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV Protocol", Elsevier, vol 79, pp 700-707, 2016

[9]. David Airehroura Jairo, A. Gutierrez, Sayan Kumar Rayc, "SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things", Elsevier, 2018

[10]. Samir Athmani, Azeddine Bilami, Djallel Eddine Boubiche, "EDAK: An Efficient Dynamic Authentication

and Key Management Mechanism for heterogeneous WSNs", Elsevier, 2017

[11]. Shehnaz T. Patel ; Nital H. Mistry, "A review: Sybil attack detection techniques in WSN", IEEE, 4th International Conference on Electronics and Communication Systems (ICECS), 2017.

[12]. Noor Alsaedi ; Fazirulhisyam Hashim ; A. Sali, "Energy trust system for detecting sybil attack in clustered wireless sensor networks", IEEE, IEEE 12th Malaysia International Conference on Communications (MICC), 2015.

[13]. T. G. Dhanalakshmi ; N. Bharathi ; M. Monisha,"Safety concerns of Sybil attack in WSN" ,IEEE, International Conference on Science Engineering and Management Research (ICSEMR)2014.

[14]. Shanshan Chen ; Geng Yang ; Shengshou Chen, "A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks", IEEE, International Conference on Communications and Mobile Computing, 2010.

[15]. Shahrzad Golestani Najafabadi ; Hamid Reza Naji ; Ali Mahani, "Sybil attack Detection: Improving security of WSNs for smart power grid application", IEEE, Smart Grid Conference (SGC), 2013.

[16]. R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, S. Lee, Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks", IEEE Transactions on Parallel and Distributed Systems, vol 20, issue 11, pp 1698–1712, 2009.

[17]. X Li, F.Zhou, J. Du, Ldts "A lightweight and dependable trust system 466 for clustered wireless sensor networks", IEEE Transactions on Information Forensics and Security, vol 8, issue 6, pp 924–935, 2013.