For Wireless Sensor Networks, a Survey of Network Security and Attack Defense Mechanisms

Mr. S. Mohammed Ibrahim, Ms. Ariya Varghese, Mr. S. Bayas Abdul Rahman, Mr. U. Dinesh, Mr. A. Mohammed Yasin,
Al-Ameen Engineering College, Erode

Abstract

Wireless sensor networks face more security challenges than traditional networks due to their harsh restrictions and demanding deployment circumstances. Several aspects of sensor networks, on the other hand, may be useful in overcoming the issue of constructing secure networks. Sensor networks' unique characteristics may offer for novel defences not present in traditional networks. We look into the security difficulties and challenges in wireless sensor networks in this research. We examine various security solutions for wireless sensor networks and identify security risks. The main objective of the paper is to present different types of Security attacks, their effects and defense mechanisms in Wireless Sensor Network which is vulnerable to security attacks and threats due to its characteristics and limitations. Security attacks are identified and classified from different perspectives e.g. based on network layer in which the attack occurs, specifically network layer wise security features and the network security basics, based on attacker location, based on transmission of information, based on different protocol stack layers etc. and the different security measures that can be applied to defend against different attacks. This survey paper focuses on various aspects of different security attacks, their effects and defense mechanisms corresponding to each attack etc.

Keywords: Wireless sensor Network, security, threat, defence, restrictions.

1.Introduction

Micro-Electro-Mechanical Systems (MEMS) technology supports the development of low cost smart sensors with limited processing and computing resources. Components of smart sensor nodes are one or more sensors, a processor, memory, a power supply, a radio, and an actuator. Battery is the main power source of a sensor node. A WSN consists of a number of sensor nodes Not only a sensor node [1-4] collects data but also have additional functionality like in-network analysis, correlation and combination of its own

sensor data and data that are coming from other sensor nodes. Many sensors cooperatively monitor large physical environments with help of a wireless sensor network (WSN). Sensor nodes take part in communication with each other and with a base station (BS) with the help of their wireless radios and it allows them to spread their sensor data for the requirement of remote processing, visualization, analysis, and storage systems.

. WSN can be of two typesStructured and Unstructured. An Unstructured WSN is one that composed of a dense collection of sensor nodes. Sensor nodes may be implemented in an ad hoc manner into the field. This type of network [5] is homogeneous in nature with respect to node type without physical hierarchy that means that they are physically and architecturally equal. In a Structured WSN, all or some of the sensor nodes are implemented in a pre-planned manner. The advantage of a Structured network is that fewer nodes can be implemented with lower network maintenance and management cost.[6]

With the introduction of the Internet of Things (IoT), the number of applications with a broad range of connections has exploded in recent years (7). The majority of IoT devices function on the concept of actuators and sensors to gather and analyze environmental data (8). This approach necessitates introducing the sensors to a variety of applications with varying degrees of broad network connectivity. (9). This issue necessitates providing the most powerful security measures capable of providing significant resiliency in the face of possible attacks across big networks (10).

It does, however, come with some possible drawbacks. The main issue is that IoT examines sensor node connections without taking into account the phenomena of WSN. This problem arises as a result of a conflict between IoT and WSN routing protocols, which employ entirely distinct methodologies (11). As a result, establishing generic safety procedures that provide equivalent capability against a specific type of threat remains a research and innovation project. The restricted capabilities of the IoT devices are a secondary concern linked with the security of WSN coupled to IoT. A sensor node is distinguished by its short battery life, low memory capacity, and inability to analyze large amounts of data sources. It's worth noting that in the WSN, there's a significant link between resource efficiency and safety protocol functioning over resource-constrained devices. A wireless sensor node utilizes energy to accomplish a variety of tasks, including operating intrinsic circuits, (ii) broadcasting and transmitting information and signals, and (iii) utilizing an information fusion approach to process the collected data (Fouad et al. 2015). But there have been a variety of research-based approaches to improving the security aspect of WSN to date, each all has its own set of flaws (12-13).

If an attacker compromises an anchor to fabricate Sybil nodes, it is considered unstable in WSN optimization. As a result, much work in WSN localization is focused on Sybil detecting attacks. (14)The signal packets traverse the same range to reach an unidentified node since Sybil identities are produced from a particular geographic point. As a result, the RSSI values measured at that unidentified node are the same for all Sybil base stations. RSSI-based schemes, such as SF-APIT (7), use RSSI values to identify Sybil attacks. RSSI values, on the other hand, fluctuate in a hostile atmosphere due to a variety of reasons such as physical barriers, signal propagation issues such as multi-path fading, and shadowing (8). As a consequence, Sybil nodes might be hidden.[15]

2.Sybil Attack

The WSN suffers from a Sybil threat while unintentionally asserting the node to some of the credentials or claims false IDs. That is, a single node might provide the network with several identities. The node duplicates itself to confuse and destabilize the network. Ind direct and direct interaction, created and stolen accounts, non-simultaneous and simultaneous threats are all examples of Sybil attacks. The Sybil attack targets the architecture, which duplicates data across multiple servers. Sybil accounts will be used to store information. Figure. 1 shows the Sybil assault, in which the adversary sites 1,2,3,4 are different ids of the base station. When these Sybil nodes wish to interact with one another, they can utilize any of the credentials. The network was confused and collapsed as a result of these illegitimately claimed nodes.

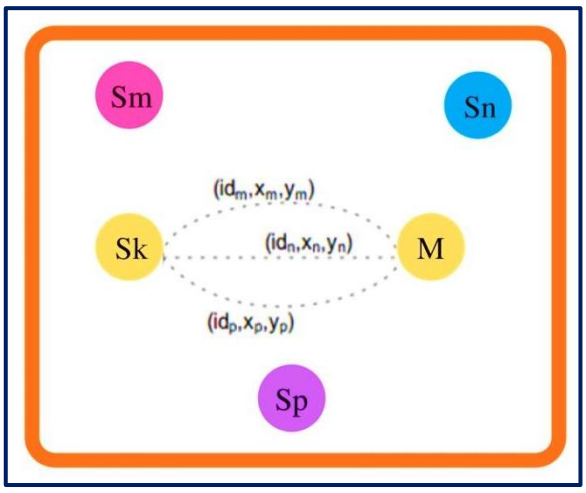

Figure.1. Attack of Sybil

2.1 Previous Works On Sybil Attacks

2.1.1. Presence Evidence System

Here, the sensor ensures that nodes on the contrary movement are actual nodes and use them as trustworthy signal intensity measurement resources. The system takes full advantage of VANET's inherent features, like high bandwidth and road layout, as well as indirect assistance from roadside infrastructure. On the other hand, Monitor discovered that by extending the observation duration, it can collect more broadcast strength data, boosting detection accuracy. This motivation has led to the development of a statistical identification approach in this paper. The statistical technique runs premise assertions and stabs on obtained measures to see if they follow a regular dispersion pattern. If the distribution pattern of a Sybil node is inaccurate when compared to its alleged physical site, it is notified. The performance of the previous system was calculated using simulations in this study. The simulations are based on accurate maps and traffic simulations from the United States [14].

2.1.2 localization principle

In the polar coordinate method, the range between different nodes is less than a tiny number; these sites are Sybil threat nodes. The networks and their geographical characteristics are then added to the blacklist. Given that a malicious network can develop anti-detection mechanisms, rule 1 (Method) can only detect a few bad nodes or cannot detect all harmful nodes. The second way is that the environment is undoubtedly pompous, but the hostile node may also be readily created by altering the signal intensity for detecting reasons, and the base station can acquire stringent coordinates in most applications [15].

Sybil assaults have a unique personality. In Sybil attacks, an anchor node (also known as a hostile anchor) is hacked to establish numerous virtual credentials. Virtual anchors all pose as the same harmful anchor. Because all virtual anchors are produced from the same physical position, their distance to M is the same, but their locations are different. As a result, all Sybil anchors have RSSI values that are almost identical to those obtained at intermediate nodes M. In other terms, Sybil anchors are all located on the same circle, which is centered at M. We presume unidentified node M is inside SK's transmission range. Because all simulated anchors sp, sm, and sn get the identical RSSI values at M, they all lie on the identical circle with M as the median.

2.1.3.Traffic Monitoring for detecting Sybil attack

This method is known as SDTM and is focused on traffic tracking. This technique does not rely on identification or location data, and it does not require any special gear. It

makes little difference if the attackers use more potent devices rather than legitimate nodes, or if the network's legitimate nodes are seized and reconfigured, turning them into attackers. This identification technique is based on the premise that the nO. of Sybil nodes in the vicinity is larger than the number of regular nodes. As a result, traffic in the vicinity of the rogue node is considerably greater [16].

2.1.4. Merkle hash tree cryptographic primitive

This paper offers an identity verification system to defend sensor networks from Sybil attacks. To build one-way key strings in this system, each sensor network is pre-assigned an individual secret code (Figure 2). The Merkle hash tree cryptographic primitive was used to distribute an identity credential to each unit, which connects its id to its one-way key chains. Any two nodes can jointly verify and certify the authenticity of their data by using a communicative node-to-node authentication mechanism. These techniques are based on symmetric key encryption as well [17].

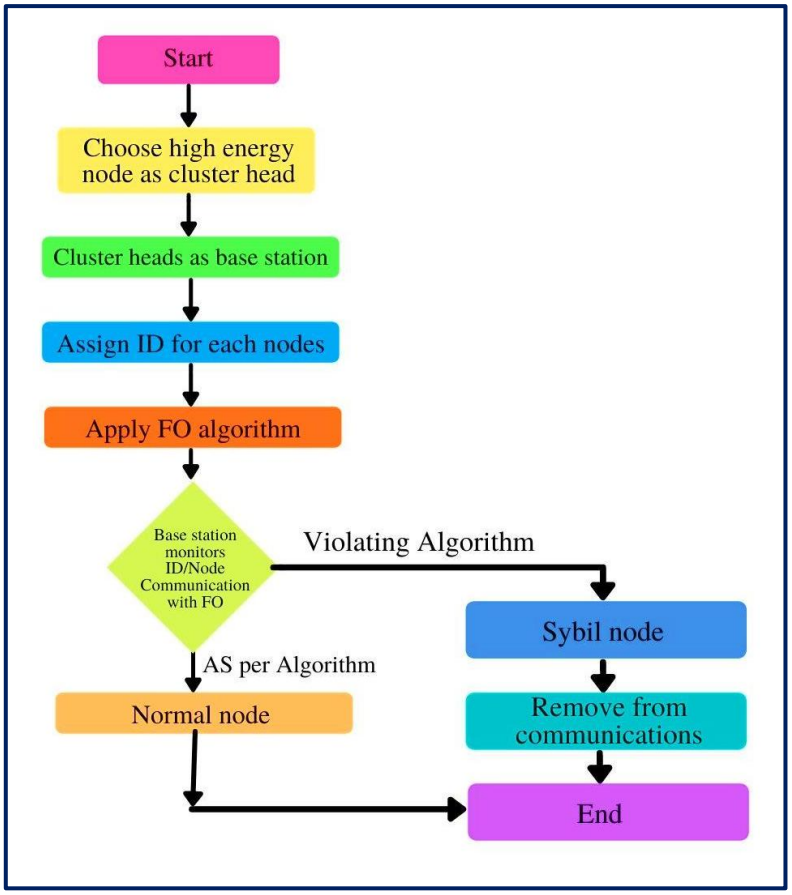

Figure.2. Flow chart

3. Proposed Method

Our suggested approach has two components. The first component is the identification of verification against the Sybil assault, and the second is Fujisaki Okamoto data validation, which preserves the quality of the information against the Sybil threat. A group of movable nodes is established when a base station is used. Each node in the network has its unique physical ID. A sensor node is a greater energy node in a collection of mobile nodes. The network IDs are all stored in the base station. The routing protocol was AODV. The base station transmits ‘hello' messages to all other units mainly for topology validation. The trust units are those that have been registered (with a unique ID) at the ground station. The trust nodes are now able to communicate with the access point.

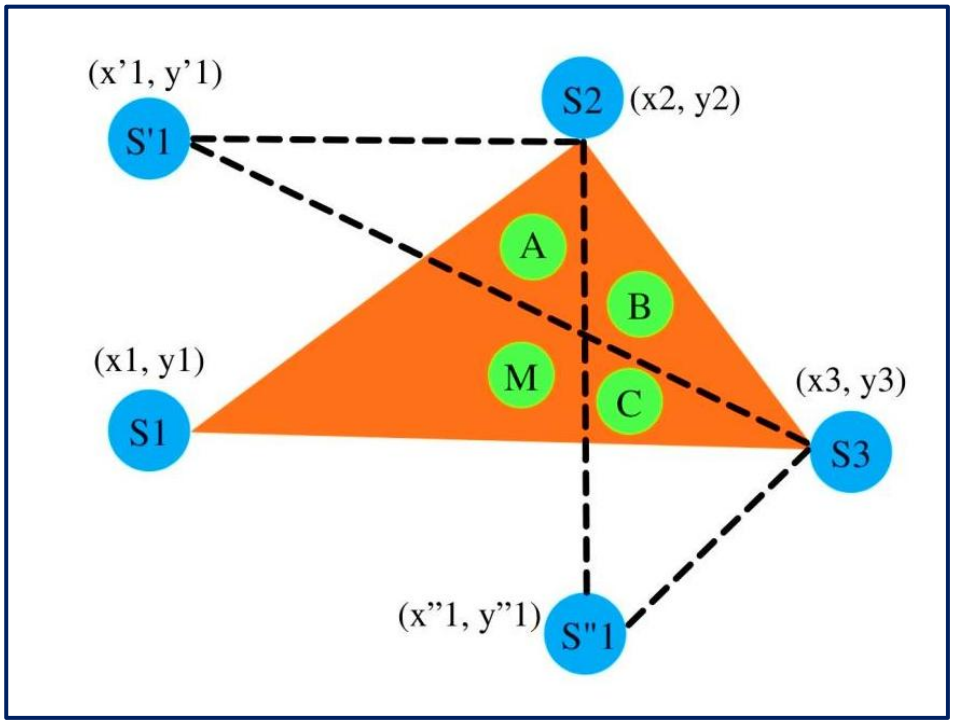

Figure.3. Node ID based FO algorithm scenario

Create a base station and a set of mobile nodes. A unique ID is meant to be assigned to each node. The member units communicate their unique ID to the access point, which verifies that they are who they say they are. The network uses the Fujisaki Okamoto method, which is a novel security transmission technique. After validating the ID, the FO algorithm is used to connect with the network (decryption and encryption).

Table 1. Parameters Of Simulation

Parameters of the simulation	
MEasurment of the area	1e+10 cm^2
Node count	59
Protocol used for transmission	UDP protocol
Measure of the packet size	512 bytes
Time used for simulation	883 seconds
Type of antenna model	Omni Direction antenna model
Category of queue	Drop trail queue
Model used for propogation	Two ray ground model for propogation
Type of traffic application	CBR
Energy during initial stage	0.51 J
Power level used for transmission in mw	0.169 mw
Power received in mw	0.169 mw
Type of protocol used for routing process	A0DV
Category of attack	Sybil attck
Algorithm used for communicating purposes	Fujisaki Okamoto

The ground station keeps an eye on the Sybil node to see if it has an ID and is incapable to interact with the FO method, which means it is excluded from all communication processes in the system, as shown in Figure. 3.

3.1 Scenario

Figure 4 depicts an instance network setup. There are 7 regular identities (1,2,3,5,6,7,8) and one (4) Sybil node, with 9 being the base station. The arrows indicate how the network's nodes communicate with one another. The grid is assigned the range 1–8, and the unit IDs are assigned accordingly by the base station(9). All other networks, except node 4, are registered with the base station.

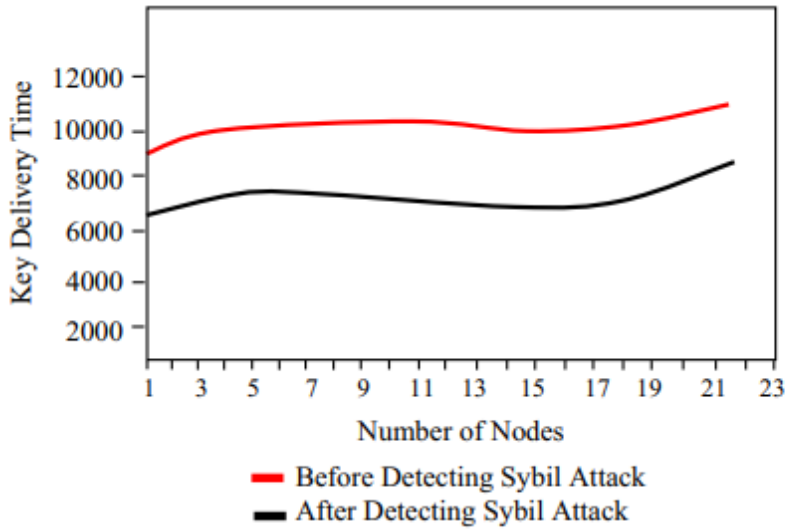

Figure.4. Broadcasting prior to Sybil attack and following it

This node will be accused of being Sybil when it communicates with the ground station. When the nodes' authenticity is examined in the second phase, it is discovered that they are unauthenticated, which indicates that node4 is verified as a Sybil node, as shown in the Figure. 5.

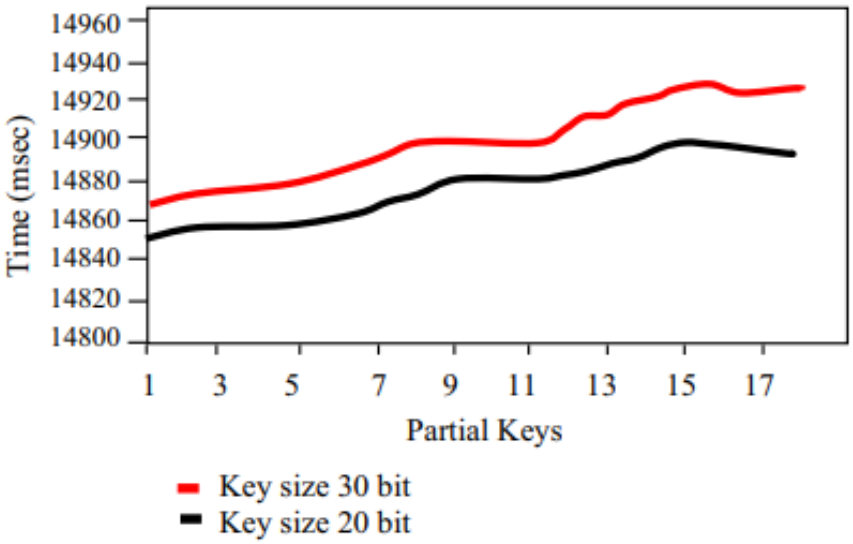

Figure.5. 20 and 30 Bits for various key sizes

4.Fujisaki Okamoto Algorithm

The identity-based method developed by Fujisaki Okamoto provides robust verification against Sybil threats. The cluster members and the ground station are responsible for decryption and encryption [18].

4.1 Performance evaluation

The efficiency of the proposed strategy is estimated using a network model in this part . The network is made up of 60 nodes that are randomly placed in a 1000 1000m2 field for this test. The app traffic was CBR , with a communication range of 250 M. The packets are 512 bytes in size and are sent four times each second. UDP is the communication protocol, whereas AODV is the routing protocol. The simulation's parameter values are listed in Tab. 1.

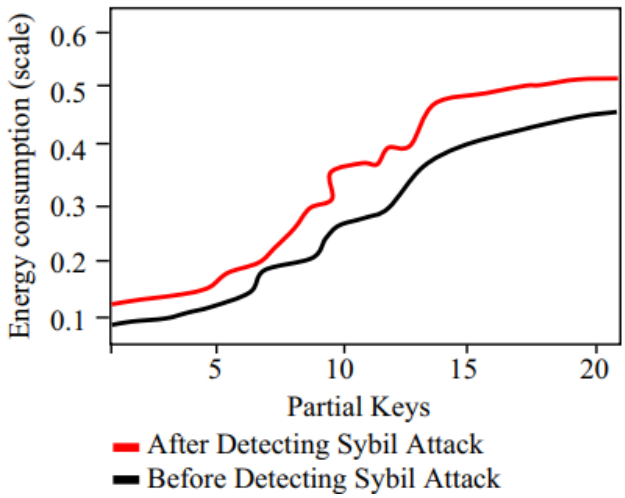

Figure.6. Consumption level of energy prior to Sybil attack

There are 60 nodes created, with node 0 serving as the ground station. To validate the architecture and start interaction, the base station transmits ‘Hello' packets. The security nodes are chosen based on their ID and assigned to communicate with the ground station. Seven of the 55 nodes are identified as Sybil nodes; once the method is run, the Sybil nodes are identified and deleted from the connection.

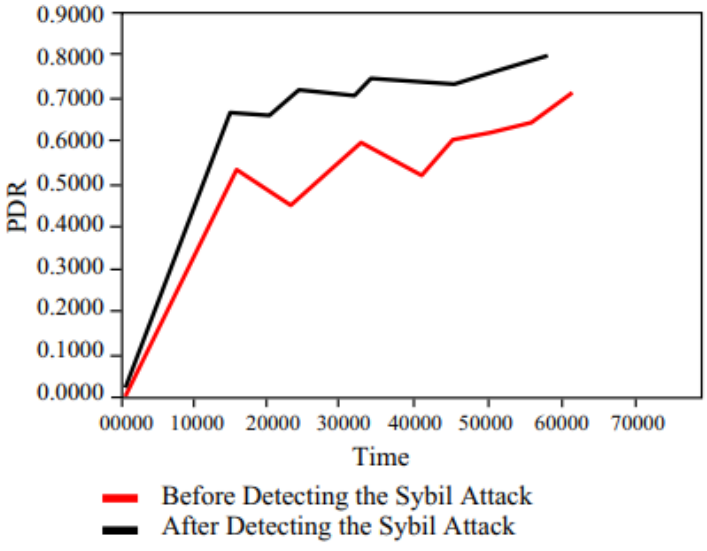

Figure.7. Network PDR prior to Sybil attack

The results for the time required for transmitting keys of size 35 and 40 bits are presented in Figure. 6. The Y-axis shows the number of incomplete keys, while the X-axis shows the time in milliseconds. The first 15 partial keys are used to compute the key transmitting in the ground station. We kept track of the time it took to generate keys of 35 and 40 bits, which differed by 20 milliseconds. The time it takes to decode one bit is potentially one second. As a result, the transmission time for a file length of 30 bits is significantly longer than for a key size of 20 bits. Figure 7 shows the network's key transmission time before and after Sybil node identification.

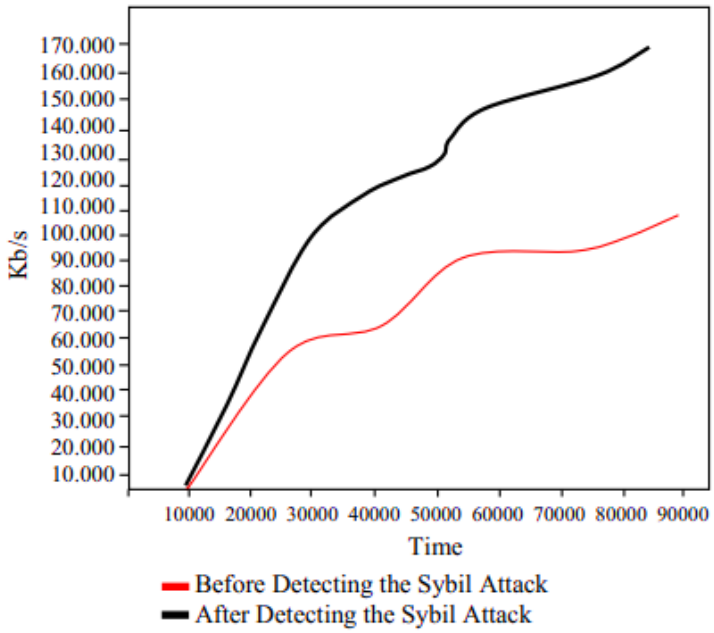

Figure.8. Network throughput prior to Sybil attack

The Y-axis represents key transmission time in milliseconds, while the X-axis represents the no. of nodes. The programming transmission time has decreased after the method was implemented (after the discovery of Sybil nodes). Figure 8 depicts the suggested model's energy usage analysis. The sensor nodes' power consumption for reception and communication was set at 32 mW, and the starting energy of the typical sensor nodes is fixed at 1 joule. Broadcasting and reception need the same amount of power, although the base station's starting energy was set at 1 joule. Figure 8 depicts the energy usage trend after and before Sybil node identification with 20-bit keys and delivery to the base s. On the Y-axis, energy is measured in joules, while on the X-axis, partial keys are measured in bits. Following the identification of Sybil nodes, the network's energy usage improves. The energy gap between after and before Sybil node identification is around 0. 170 J. Figure 7 shows a

study of the network's PDR before and after the algorithm's deployment. The X-axis measures time in milliseconds and the Y-axis measures PDR. This shows that after adopting the method, the PDR improves and the Sybil nodes are removed from the network. Figure 8 shows a comparison of performance after and before the method was implemented. The X-axis represents time, whereas the Y-axis represents throughput in kb/s. The network's throughput is low due to the existence of the Sybil nodes, as can be observed from the chart. The figure also shows that after running the method, the Sybil nodes are removed from the network. As a result, there is a high flow.

5. Conclusions:

Because of the wide range of security-critical wsn applications, security is becoming a serious concern for energy-constrained wireless sensor networks. As a result, WSN security has received a lot of attention in recent times. Because of the unique characteristics of WSNs, designing good security protocols with low overheads is extremely difficult. We've covered several security challenges, risks, and assaults in WSNs, as well as potential solutions, in this paper. WSN network security is still a promising research area that should be pursued further.

References:

[1] J. Parras and S. Zazo, “Learning attack mechanisms in wireless sensor networks using Markov decision processes,” Expert Syst. Appl., vol. 122, pp. 376–387, 2019.

[2] A.-u. Rehman, S. U. Rehman, and H. Raheem, “Sinkhole attacks in wireless sensor networks: a survey,” Wireless Pers. Commun., vol. 106, no. 4, pp. 2291–2313, 2019.

[3] G. Farjamnia, Y. Gasimov, and C. Kazimov, “Review of the techniques against the wormhole attacks on wireless sensor networks,” Wireless Pers. Commun., vol. 105, no. 4, pp. 1561–1584, 2019.

[4] J. Jiang et al., “A survey on location privacy protection in wireless sensor networks,” J. Netw. Comput. Appl., vol. 125, pp. 93–114, 2019.

[5] G. Yang et al., “Challenges and security issues in underwater wireless sensor networks,” Procedia Comput. Sci., vol. 147, pp. 210–216, 2019.

[6] H. Xie et al., “Data collection for security measurement in wireless sensor networks: A survey,” IEEE Internet Things J., vol. 6, no. 2, pp. 2205–2224, 2018.

[7] S. Pundir et al., “Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: survey and future challenges,” IEEE Access, vol. 8, pp. 3343–3363, 2019.

[8] X. Ge et al., "Distributed event-triggered estimation over sensor networks: A survey," IEEE Trans. Cybern., vol. 50, no. 3, pp. 1306–1320, 2019.

[9] R. W. Anwar et al., "BTEM: Belief based trust evaluation mechanism for wireless sensor networks," Future Gener. Comput. Syst., vol. 96, pp. 605–616, 2019.

[10] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," IEEE Access, vol. 7, pp. 33859–33869, 2019.

[11] M. S. Abdalzaher, L. Samy, and O. Muta, "Non-zero-sum game-based trust model to enhance wireless sensor networks security for IoT applications," IET Wireless Sensor Syst., vol. 9, no. 4, pp. 218–226, 2019.

[12] A. Balueva, V. Desnitsky, and I. Ushakov, "Approach to detection of Denial-of-Sleep attacks in wireless sensor networks on the base of machine learning," in Proc. Int. Symp. Intell. Distrib. Comput., Cham, Switzerland: Springer, 2019.

[13] J. P. Walters et al., "Wireless sensor network security: A survey," in Security in Distributed, Grid, and Pervasive Computing, X. Yang, Ed., 2006.

[14] A. I. Al-Issa et al., "Using machine learning to detect DoS attacks in wireless sensor networks," in Proc. IEEE Jordan Int. Joint Conf. Electr. Eng. Inf. Technol. (JEEIT), 2019.

[15] V. Nagireddy and P. Parwekar, "Attacks in wireless sensor networks," in Smart Intelligent Computing and Applications, Singapore: Springer, 2019, pp. 439–447.