International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 10, October 2017
www.ijarse.com
IJARSE
ISSN 2319 - 8354

Survey on Literature Detection Methods of Sybil Attack in WSN

Omar Badeea Baban[1]

[1]*Department of Computer Engineering, Sinhgad College of Engineering, Pune-41, Pune, (India)*

ABSTRACT

A wireless Sensor Network (WSN) is a distributed network of small sensor nodes deployed in large numbers to monitor the environment or other systems by the measurement of physical parameters such as temperature, pressure, or relative humidity. These nodes by monitoring collect detailed information about the physical environment in which they are installed, and then transmit the collected data to the Base Station (BS). BS is a gateway from sensor networks to the outside world. The BS has a very large storage and large data processing capabilities. It passes the data it receives from sensor nodes to the server from where end-user can access them. Security in WSN is a greater challenge due to the processing limitations of sensor nodes and nature of wireless links. Extensive use of WSNs is giving rise to different types of threats. To defend against the threats proper security schemes are required. Traditionally security is implemented through hardware or software and is generally achieved through cryptographic methods. Limited area, nature of links, limited processing, power and memory of WSNs leads to strict constraints on the selection of cryptographic techniques.

The Sybil attack is one of the dangerous attacks against sensor and ad-hoc networks, where a node illegitimately claims multiple identities. A Sybil attacker can cause damage to the ad hoc networks in several ways. For example, a Sybil attacker can disrupt location-based or multipath routing by participating in the routing, giving the false impression of being distinct nodes on different locations or paths. In reputation and trust based misbehavior detection schemes, a Sybil node can disrupt the accuracy by increasing its reputation or trust and decreasing others' reputation or trust by exploiting its virtual identities. In wireless sensor networks, a Sybil attacker can change the whole aggregated reading outcome by contributing many times as a different node. In voting-based schemes, a Sybil attacker can control the result by rigging the polling process using multiple virtual identities. In vehicular ad hoc networks, Sybil attackers can create an arbitrary number of virtual nonexistent vehicles and transmit false information in the network to give a fake impression of traffic congestion in order to divert traffic.

Keywords Wireless Sensor Network, Sybil Attack, Sensor, illegitimately, Clusters, Cluster Head, Vulnerable, Base Station.

I. INTRODUCTION

1.1 Motivation

A wireless sensor network (WSN) is a network formed by a large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSNs are regarded as a revolutionary information gathering method to build the information and communication system which will

greatly improve the reliability and efficiency of infrastructure systems. Compared with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

Today, smart grid, smart homes, smart water networks, intelligent transportation, are infrastructure systems that connect our world more than we ever thought possible. The common vision of such systems is usually associated with one single concept, the internet of things (IoT), where through the use of sensors, the entire physical infrastructure is closely coupled with information and communication technologies; where intelligent monitoring and management can be achieved via the usage of networked embedded devices. In such a sophisticated dynamic system, devices are interconnected to transmit useful measurement information and control instructions via distributed sensor networks.

Node's identities are used as an address to communicate with a network entity. This forms a one-to-one mapping between an identity and an entity. Usually, the identity is assumed either implicitly or explicitly by many protocol mechanisms; hence two identities imply two distinct nodes. Unfortunately malicious nodes can illegitimately claim multiple identities and violate this one-to-one mapping. Douceur [7] termed this as a Sybil attack, in which an attacker manages to create and control more than one identity on a single physical device.

The traditional approach to prevent Sybil attacks is to use cryptographic-based authentication or trusted certification. However, this approach is not suitable for mobile ad hoc networks because it usually requires costly initial setup and incurs overhead related to maintaining and distributing cryptographic keys. On the other hand, received signal strength (RSS) based localization is considered one of the most promising solutions for wireless ad hoc networks. However, the traditional technique requires Geographical positioning system and Hardware like antennas, so the cost of the initial setup is very high. This paper describes, differentiation of legitimate user and illegitimate user or Sybil attacker even in the high mobility because, now a days the QOS is necessary in the network. This proposed scheme detects Sybil identities and legitimate identity even in high mobility. In particular, proposed scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First, we demonstrate the entry and exit behavior of legitimate user and Sybil user using simulation and real world test bed experimentation. Second, the threshold is defined to distinguish between the legitimate node and the Sybil node based on nodes' entry and exit behavior. Third, the threshold is detected by the getting average of all the nodes received signal strength values.

1.2 Definitions of WSN

A WSN can generally be described as a network of nodes that cooperatively sense and control the environment, enabling interaction between persons or computers and the surrounding environment.

WSNs nowadays usually include sensor nodes, actuator nodes, gateways and clients. A large number of sensor nodes deployed randomly inside of or near the monitoring area (sensor field), form networks through self-organization. Sensor nodes monitor the collected data to transmit along to other sensor nodes by hopping. During the process of transmission, monitored data may be handled by multiple nodes to get to gateway node after multichip routing, and finally reach the management node through the internet or satellite. It is the user

who configures and manages the WSN with the management node; publish monitoring missions and collection of the monitored data.

As related technologies mature, the cost of WSN equipment has dropped dramatically, and their applications are gradually expanding from the military areas to industrial and commercial fields. Meanwhile, standards for WSN technology have been well developed, such as Zigbee, Wireless Hart, ISA 100.11a, wireless networks for industrial automation – process automation

(WIA-PA), etc. Moreover, with new application modes of WSN emerging in industrial automation and home applications, the total market size of WSN applications will continue to grow rapidly.

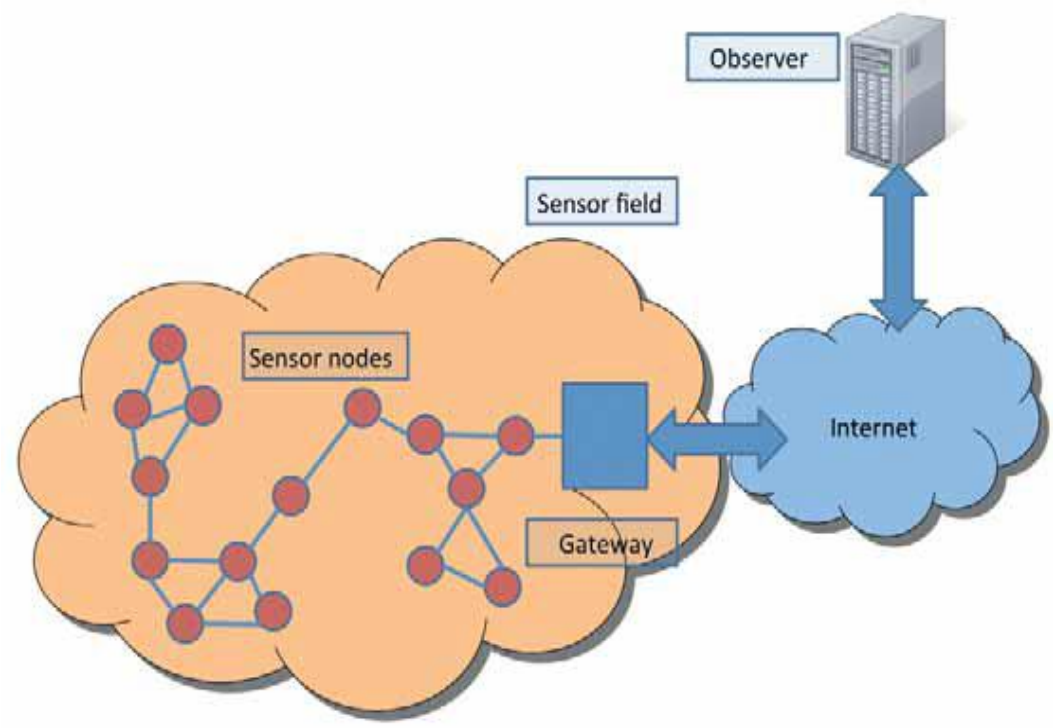

Figure 1.1 Wireless Sensor Networks [5]

The sensor node is one of the main parts of a WSN.

The hardware of a sensor node generally includes four parts: the power and power management

module, a sensor, a microcontroller, and a wireless transceiver, see Figure 1.2.

The power module offers the reliable power needed for the system.

The sensor is the bond of a WSN node which can obtain the environmental and equipment status. A sensor is in charge of collecting and transforming the signals, such as light, vibration and chemical signals, into electrical signals and then transferring them to the microcontroller. The microcontroller receives the data from the sensor and processes the data accordingly. The Wireless Transceiver (RFmodule) then transfers the data, so that the physical realization of communication can be achieved.

It is important that the design of the all parts of a WSN node consider the WSN node features of tiny size and limited power.

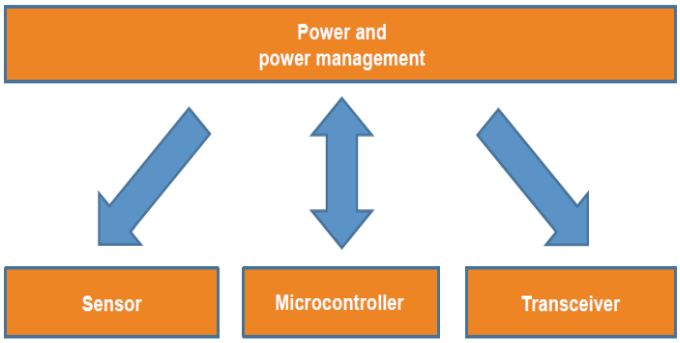

Figure 1.2 Hardware Structure of a WSN sensor node [5]

A wireless sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment.WSN is a very large array of diverse sensor nodes that are interconnected by a communication network. The sensing data are shared between the sensor nodes and are used as input for a distributed estimation system. The fundamental objectives for WSN are reliability, accuracy, flexibility, cost effectiveness, and ease of deployment. WSN is made up of individual multifunctional sensor nodes.

Organization of large multi-hop wireless networks into clusters is essential for achieving basic network performance. In wireless sensor networks (WSN), the clustering is primarily characterized by data aggregation by each cluster head, which significantly reduces the traffic cost. The hierarchical model requires two main methods: Periodic selection of cluster heads (CHs) and Assignment of each node to one or multiple clusters.

Sybil Attack Definitions

Sybil node is the process of creating two or more duplicate nodes with similar identity i.e. same node id as shown in Fig.1.3. Particularly, wireless sensor networks are more prone to Sybil attack because of the open and broadcast communication medium and the same frequency is being shared among all nodes. In Sybil attack, attacker makes multiple illegitimate identities in sensor networks either by fabricating or stealing the identities of legitimate nodes. So the base station cannot distinguish the legitimate and the forged node. This confuses the base station and other nodes and the network performance degrades.

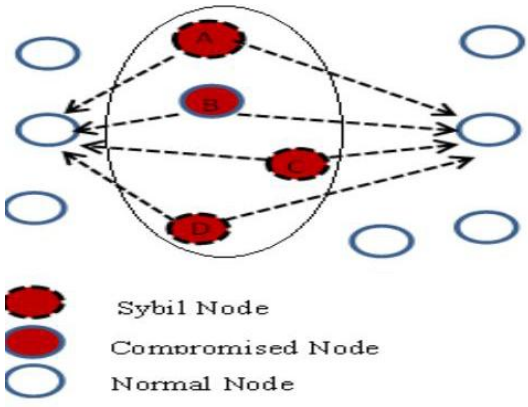

Figure 1.3 Sybil Node [17]

In Wireless sensor networks, mechanisms for redundancy are identity-based. It is assumed that each node is distinguished as one entity and presents only one single abstract concept of an identity. Hence, WSNs. and nodes are vulnerable to any method which allows identities to be forged or falsified. Such a malicious method is the Sybil attack. In Sybil attack, a single node intentionally, illegally presents many false or forges identities to other nodes in the network by either new (false) identities, or stealing legal identities from others. A Sybil node is a misbehaving node's extra identity. Therefore, a single entity may get selected many times (depends on number of identities) to participate in an network operation that relies on redundancy, thereby controlling the outcome of the operation, and defeating the redundancy mechanisms.

Doueceur introduced the Sybil attacks on P2P architecture first time [7]. Roosta ET. Al. also presented their views on variety and defense mechanisms against Sybil attacks [27]. Detailed analysis of Sybil attack was also proposed by Cemtepe and Yener. [24]

Sybil attack can take place while broadcasting without any central authority. This central authority may help in identifying the identities of nodes. Attacker can have different identities by sending messages with multiple identifiers. When a node illegitimately claims many identities or having multiple stolen identities, WSN suffers from Sybil attack. The such malicious sensor node itself replicates its multiple copies to damage the network. There can be Sybil attack internally or externally. Authentication may somehow prevent from external attacks but not from

internal. One of important observation about Sybil attack is that it attacks on the violation of one-to-one mapping between identity and entity in WSN. [25]

A. Types of Sybil attack

For detecting the Sybil attack it is necessary to understand the different forms in which the network is attacked:

1) Direct and Indirect Communication: In direct type of attack, the legitimate nodes communicate directly with the Sybil nodes whereas in indirect attack, the communication is done through the malicious node.

2) Fabricated and stolen identities: In this type of attack, malicious node creates a new identity for itself based on the identities of the legitimate nodes. When these malicious nodes want to communicate to their neighboring nodes they use any one of the fake identities. This result in confusion and collapses the network. In stolen identities, attacker first identifies legitimate identities and then uses it. This type of attack may go unidentified in the case the node whose identity has been stolen is destroyed. Identity replication is done when the same identities are used number of times in the same places.

3) Simultaneous and non-simultaneous attack: In simultaneous attack, all the Sybil identities participate at the same time in the network. Due to only one identity appearing at a time, cycling through identities will make it to appear simultaneous. In non – simultaneous attack, the number of identities the attacker uses is equal to the number of physical devices present where each device presents different identities at different times.

1.3 Why Security in WSN

Wireless Sensor Network (WSN) is a distributed network and it comprises a large number of distributed, self-directed, tiny, and low powered devices called sensor nodes alias motes. WSN naturally encompasses a large

number of spatially dispersed, petite, battery-operated, embedded devices that are networked to supportively collect, process, and convey data to the users, and it has restricted computing and processing capabilities.

Nowadays wireless network is the most popular services utilized in industrial and commercial applications, because of its technical advancement in processor, communication, and usage of low power embedded computing devices. Sensor nodes are used to monitor environmental conditions like temperature, pressure, humidity, sound, vibration, position etc. In many real time applications the sensor nodes are performing different tasks like neighbor node discovery, smart sensing, data storage and processing, data aggregation, target tracking, control and monitoring, node localization, synchronization and efficient routing between nodes and base station.

Securing network protection in Wireless Sensor Networks (WSNs) increasingly becomes critical. There are many attacks that have been recognized in WSN till now by the researchers. Sybil attack is one of the harmful attacks against sensor network where a number of legitimate identities and forged identities are used to get an illegitimate entry into the network. Basically a Sybil attack means a node which pretends its identity like other nodes. In this scenario a node can trust the pretend node and it start sharing its information. Due to this activity a node's security is affected and information is lost.

Many security mechanisms against security threats in WSNs. have been deployed for many years, but no any effective solutions regarding the implementation of same have been found out till time.

WSN's general security goals are confidentiality, integrity, authentication, availability, survivability, efficiency, freshness and scalability as described below.

WSN is susceptible to many attacks because of its transmission nature, resource restriction on sensor nodes and deployment in uncontrolled environments. To ensure the security services in WSN many crypto mechanisms like symmetric and asymmetric methods are proposed. To achieve security in wireless sensor networks, it is important to be able to encrypt and authenticate messages sent between sensor nodes.

1. Confidentiality Keeping node information secret from others but authorized users see it.
2. Integrity Possible for the receiver node of a message to confirm that it has not been customized in transit.
3. Device authentication Justification of the identity of the device.
4. Message authentication Justification the source of information.
5. Validation to provide correctness of authorization to use or manipulate resources.
6. Access control Restricting access to resources.
7. Revocation Renunciation of certification or authorization.
8. Survivability The lifetime of the sensor node must be extended even the node is compromised.
9. Non repudiation preventing the denial of a previous commitment.
10. Availability High availability systems in sensor node is aim to remain available at all times preventing service disruptions due to power outages, hardware failures, and system upgrades.

Ensuring availability also involves preventing denial-of-service attacks.

11. Data freshness Data freshness objective ensures that messages are fresh, meaning that they are in proper order and have not been reused. [8]

II. LITERATURE REVIEW

2.1 Literature Detection methods of Sybil Attack in WSN

Still now there exists no such well accepted technique to detect the Sybil attack. A number of methods have been proposed associated with different environments. Some of them are effective to reduce the threat to a satisfactory level. In this section different approaches proposed to prevent and mitigate the attack are discussed.

A. Message Authentication and Passing Method According to authors in [30], the Sybil attack is a massive destructive attack against the WSN, in which numerous genuine identities with forged identities are used for getting an illegal entry into a network. The existing method Random Password Comparison has only a scheme which is to just verify the node identities by analyzing the neighbors. In this paper authors, proposed a scheme of assuring the security for wireless sensor network, to deal with the attacks of these kinds in unicasting and multicasting. In this paper the message authentication and passing method is applied in order to check the trustworthiness or otherwise for a Sybil node. Verification of node needs the application of CAM-PVM. Instead of wasting time for CAMPVM to check each node, the message authentication and passing procedure is to be applied for authentication prior to communication. If a node does not have any authorization from the network or from the base station, it can't communicate with any other node in the network. The message authentication and passing method is known for more time consuming as compare to any other method.

B. TDOA method Authors emphasize on sybil attack and proposed an algorithm for sybil attack detection based on Time difference of Arrival (TDOA) localization method in [26]. This method detects the malicious behavior of head node and member nodes in a cluster based network. In this paper, authors, proposed a method to detect the head node and member node of cluster in WSN as sybil. Authors claim that in comparison to the conventional sybil attack detection methods, their TDOA based approach is better as it does not require any computational overhead to sensor nodes. According to authors, TDOA has achieved a detection rate of 96% along with very low false positive rate of 4%. The paper also analyze the consumption of energy of nodes before and after attack. In order to minimize the consumption of energy, an energy efficient algorithm has been suggested in the paper.

C. Random password comparison method A Random Password Comparison [RPC] method is proposed in [18]. This method facilitates deployment and control of the positions of the nodes and thereby it prevents the occurrence of sybil attack in WSN. According to authors, the RPC method is dynamic as well as accurate in detecting the sybil attack. The method also helps in improving data transmission in the network along will increase in the throughput. RPC algorithm discovers a valid route in the sensor network by checking each node is a trustable node or a sybil node so that the data can be transmitted very safely. The authors claim that, the sybil nodes are detected and data leakage is avoided completely by using RPC. As the sybil nodes are detected in the discovery stage of finding initial route, this enables continuation of the for further transmission without any fear of attack.

D. Neighborhood RSS based approach Investigation of Sybil attack which is one of the most disrupting attacks in context of wireless sensor networks is done in [31]. A lightweight scheme is proposed in this paper to detect the new identities of sybil nodes, this scheme does not use centralized trusted third party, it makes use of neighborhood RSS to differentiate between the legitimate and Sybil identities. RSS based process is used in this

paper to detect Sybil attacks in a wireless sensor network. According to authors, it is verified that a detection threshold is used to make the distinction between legitimate new nodes and new malicious identities.

Throughput, packet loss ratio, true positive rates, end-to-end delay, false positive rates are used to analyze the performance of the system. According to authors, the simulation results show that this scheme has a high level of accuracy with detection process gives us the high true positive rates up to 80% with low false positive rates that range to 16%.

E. SYBILSECURE technique An energy efficient algorithm named Sybil Secure is proposed in [1]. According to the authors, experimental results show that Sybil secure consumes less energy as compare to the existing defense mechanisms. Sybil secure is based on sending and acknowledging the query data packets. Social network based schemes that are involved in random routes of data consume more energy in order to detect a sybil node. But in Sybil secure , less energy is used for detection of Sybil node. The proposed solution is basically based on sending to and responding from the query sent by the cluster head. The Cluster head has a list of its sub nodes parameters, these parameters are identities and their locations. The Cluster head broadcasts query packet to all sub-nodes in such a way that it expects a reply from all the sub nodes, so that they must send their id and location.

F. Genetic algorithm Authors aimed to select nodes for clustering using LEACH-EGA in [19]. This is done in order to improve the energy efficiency with trusted nodes. Before, the clustering in the sensor network, all the nodes are optimized with the help of Genetic algorithm. LEACH-E is used for clustering and CH election. The nodes are optimized with the help of attributes such as energy value, trust value, distance etc. According to authors, from the experimental results, it is clear that the proposed LEACH-E-GA is efficient in terms of energy saving and security. This algorithm provides more effective output as proved from the graphs and tables in the paper. The packet loss is also reduced in the proposed approach by using Genetic algorithm. This enables the sensor network to continue with their transmission without any delay and fear of attack.

G. Two-hop messages approach A distributed and efficient algorithm is proposed in [21] based on broadcasting two-hop messages. This approach is used to detect sybil nodes in wireless sensor networks. In the proposed algorithm by authors, by sending two hop messages, each node finds its two hop neighbors and common neighbors between itself and each of its two hop neighbors. The number of common neighbors is one of the good indicators to detect Sybil nodes. The proposed algorithm has been simulated in ns2 and its efficiency has been compared with other available algorithms. Experimental results by authors show that the proposed algorithm outperforms similar other existing algorithms with respect to true and false detection rates. This paper presents a dynamic, distributed algorithm for the detection of sybil nodes in wireless sensor networks.

H. P2DAP approach A lightweight and scalable protocol to detect sybil attacks is provided in [28]. According to authors, Vehicular adhoc networks (VANETs) are being increasingly used for traffic control, management of parking lots, accident avoidance, and public areas. Two major concerns in VANETs are security and privacy. In VANETs, most privacy-preserving schemes are vulnerable to sybil attacks, in which a malicious user can pretend to be multiple vehicles. In the proposed scheme, malicious node can be detected in a distributed manner. This is done through passive overhearing by set of fixed nodes called road-side boxes (RSBs). The detection of sybil attacks does not require any vehicle to disclose its identity in the network; hence privacy is preserved for at

all times. Simulation results are presented by authors, for a realistic test case in order to highlight the overhead for a centralized authority. The results by authors also quantify the inherent trade-off between securities, i.e., the detection of sybil attacks and detection latency, and the privacy provided to the vehicles in the network. From the results, it is clear that proposed scheme being able to detect sybil attacks at low delay and overhead, while preserving privacy of vehicles.

I. TIME-TO-TIME MESSAGE model A scheme called TIME-TO-TIME MESSAGE (TTM) model to detect the sybil attack in wireless sensor network is proposed in [2]. Every node in the WSN will maintain the observation table, used for storing node id along with location to detect the sybil node. The simulation results by author showed that the detection of sybil attack is high in sensor network. The communication overhead is also less as compared with other existing algorithms. In this paper, observation table is used to detect the sybil nodes accurately. The simulation results are also compared with other existing similar methods and it shows that TTM approach is having a good efficiency in terms of speed and detection time. The main advantage of this proposed algorithm is that while receiving the packets, each node store the id and location in order to detect the malicious node.

J. Compare and Match Approach A survey is done on sybil attack and a Compare and Match (CAM) approach is proposed in [29]. The approach is used to verify the Position to prevent sybil attacks. In this paper authors outlined CAM algorithm for prevention of sybil attack in wireless sensor network. A malicious node can be a sybil node if and only if it knows the complete information about the other nodes. A sybil node can have any duplicate ID and duplicate information after obtaining this information. CAM approach can be used for the verification of node. A node can only communicate with other nodes after authorization by the network or from base station. According to authors, CAM is very effective and efficient as compare to other existing methods.

K. Energy and Hop based Detection An Energy and Hop-Distance (EH) based detection of Sybil attack for Mobile Wireless Sensor Network is proposed in [23]. The detection of malicious node is done in three phases, where in the first phase of method the node energies are compared with the threshold value. In the second phase the distance between suspected sybil nodes is calculated and finally, the route followed by the packets are checked for confirmation of a sybil node. The performance of the proposed scheme is analyzed and the simulation results are compared by authors with the existing methods. It is observed from the results that, the proposed scheme increase the Packet delivery ratio along with throughput of the network. The energy consumed by this algorithm is 3.4 Joules. Most of existing detection schemes are based on RSSI, a novel method of the detecting of Sybil attack based on energy, and hop-distance. Every node in the network checks its energy level. Further nodes are detected based on the distance and hop. The accuracy of the proposed detection method is high with less overhead. The scheme detects multiple sybil nodes in the sensor network. Since these nodes are mobile nodes, there will be less false positives. This could result in the node to misbehave in the network.

L. Thershold Elgamal Key Management Scheme After analyzing the problems related with existing security schemes of WSN, authors propose a model that allow to distinguish between legal nodes and malicious nodes in sensor networks to prevent the sybil attack in [9]. To defend against the sybil attack proposed scheme validate each node identity to the only identity presented by the corresponding physical node.

There are basically two ways to validate an identity. The first type is the direct validation in which a node directly tests another node identity. The second type is indirect one in which already verified nodes allowed to vouch for or refute other nodes. In the proposed approach Elgamal based key management scheme is used. The Elgamal encryption scheme is an asymmetric key encryption algorithm used for public-key cryptography, which is based on the Diffie–Hellman key exchange. A Threshold ElGamal-based key management scheme is used in this paper for protection against sybil attack. Forge identities detection is required for the early decisions like verifications of the user's intention at the time of profile creations. This can be achieved by the historical transmission activity details analyzed in real time. These activities require heavy processing requirements.

M. Optimized secure routing protocol A security based on LEACH routing protocol against Sybil attack is proposed in [14]. The mechanism used in the paper is set up to detect sybil attack based on the distance and hop count between the nodes. The prevention is done based on encryption technique which uses unique identities of the nodes. The authors also calculate performance parameters energy consumption. The results show the efficiency of the proposed protocol. The proposed work help in preventing the wireless sensor network from the security risk due to sybil attack. The encryption technique used in the paper is based on the binomial distribution.

N. RSSI-based Scheme Authors present a robust and lightweight solution in [15] for sybil attack problem. The solution is based on received signal strength indicator (RSSI) which is used for readings of messages. Authors claim that their solution is robust as it detects all sybil attack cases with less than a few percent false positives. The solution in the paper is lightweight in the sense that it alongside the receiver need the collaboration of one other node. Authors show through experiments that even though RSSI is time-varying and unreliable, using ratio of RSSIs from multiple receivers, it is feasible to overcome these problems.

O. Channel-Based Detection An enhanced physical-layer authentication scheme to detect sybil attacks is proposed in [11]. This exploits the spatial variability of radio channels in the environments with rich scattering. Authors build a hypothesis test in order to detect sybil clients for both narrowband and wideband wireless systems, Based on existing channel estimations mechanisms, proposed method can be easily implemented with low overhead. This can be done either independently or combined with other physical-layer security methods. The performance of proposed sybil detector in the paper is verified, via both a propagation modeling software. A field measurement using a vector network analyzer is also used for typical indoor environments. Authors claim that their evaluation examines numerous combinations of system parameters such as bandwidth, number of channel estimates, signal power, number of total clients, number of sybil clients, and number of the access points. According to authors, both the false alarm rate and the miss rate of sybil attacks are below 0.01, pilot power of 10 mW, with three tones, and a system bandwidth of 20 MHz.

P. UWB ranging-based information A novel rule-based sybil attack detection system for large-scale WSNs is proposed in [19]. Integration of UWB ranging features with expert knowledge is used for the detection process. Paper proposes development of a defense scheme against direct, simultaneous sybil attacks with derivation of a rigorous analytic framework for the determination of the system performance. Paper use accurate simulation environment to validate the detection analysis. This work restrains its focus on defending against a particularly harmful form of attack, the sybil attack. This paper focus on a rule-based anomaly detection system. This system

is called RADS, which monitors and timely detects Sybil attacks in large-scale WSNs. The proposed expert system relies on an ultra-wideband (UWB) ranging-based detection algorithm. This algorithm usually operates in a distributed manner that requires no information sharing or cooperation between the sensor nodes in order for performing the anomaly detection tasks. In the paper feasibility of the proposed scheme is proven analytically. The performance of RADS in exposing sybil attacks is extensively assessed both numerically or mathematically. According to authors, the obtained results demonstrate that RADS achieves high detection accuracy along with low false alarm rate. [20]

2.2.Survey Conclusion

In this section different proposed approaches to prevent and mitigate the Sybil attack are discussed and their comparative study is represented in Table 2.1.

Table 2.1: Comparative Analysis of the Techniques to Prevent and Mitigate the Sybil attack and Their Disadvantages [20].

Technique to mitigate Sybil attack	Disadvantages / Limitations
Message Authentication and Passing Method	• The message authentication and passing method is applied in order to check the trustworthiness or otherwise for a Sybil node or otherwise for a Sybil node. • If a node does not have any authorization from the network or from the base station, it can't communicate with any other node in the network. • The message authentication and passing method is known for more time consuming as compare to any other method.
TDOA method	• It is an algorithm for Sybil attack detection based on Time difference of Arrival (TDOA) localization method. • This method detects the malicious behavior of head node and member nodes in a cluster based network. • TDOA has achieved a detection rate of 96% along with very low false positive rate of 4%. • It doesn't require any computational overhead to sensor nodes. • Minimize the nodes consumption of energy during an attack.
Random password comparison method	• This method facilitates deployment and control of the positions of the nodes and thereby it prevents the occurrence of Sybil attack in WSN, the RPC method is dynamic as well as accurate in detecting the Sybil attack. • RPC algorithm discovers a valid route in the sensor network by checking

	each node is a trustable node or a Sybil node so that the data can be transmitted very safely. • The Sybil nodes are detected and data leakage is avoided completely by using RPC.
Neighborhood RSS based approach	• This lightweight scheme use of neighborhood RSS to differentiate between the legitimate and Sybil identities. • This scheme has a high level of accuracy with detection process gives us the high true positive rates up to 80% with low false positive rates that range to 16%.
SYBILSECURE technique	• Experimental results show that Sybil secure consumes less energy as compare to the existing defense mechanisms. • Sybil secure is based on sending and acknowledging the query data packets. • The proposed solution is basically based on sending to and responding from the query sent by the cluster head. The Cluster head has a list of its sub nodes parameters, these parameters are identities and their locations. The Cluster head broadcasts query packet to all sub-nodes in such a way that it expects a reply from all the sub nodes, so that they must send their id and location.
Genetic algorithm	• LEACH-E is used for clustering and CH election. The nodes are optimized with the help of attributes such as energy value, trust value, distance etc. • From the experimental results, it is clear that the proposed LEACH-E-GA is efficient in terms of energy saving and security. This algorithm provides more effective output as proved from the graphs and tables. • The packet loss is also reduced in the proposed approach by using Genetic algorithm. This enables the sensor network to continue with their transmission without any delay and fear of attack.
Two-hop messages approach	• This algorithm is based on broadcasting two-hop messages • In this algorithm by sending two hop messages, each node finds its two hop neighbors and common neighbors between itself and each of its two hop neighbors. The number of common neighbors is one of the good indicators to detect Sybil nodes. • Experimental results by authors show that the proposed algorithm outperforms similar other existing algorithms with respect to true and false detection rates.
PDAP approach	• This algorithm is used in Vehicular adhoc networks (VANETs), In VANETs; most privacy-preserving schemes are vulnerable to Sybil attacks, in which a malicious user can pretend to be multiple vehicles. • In the proposed scheme, malicious node can be detected in a distributed

	manner. This is done through passive overhearing by set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks does not require any vehicle to disclose its identity in the network; hence privacy is preserved for at all times. • From the results, it is clear that proposed scheme being able to detect Sybil attacks at low delay and overhead, while preserving privacy of vehicles.
TIME-TO-TIME MESSAGE model	• Every node in the WSN will maintain the observation table, used for storing node id along with location to detect the Sybil node. • The simulation results by author showed that the detection of Sybil attack is high in sensor network. The communication overhead is also less as compared with other existing algorithms.
Compare and Match Approach	• This approach is used to verify the Position to prevent sybil attacks. • A malicious node can be a sybil node if and only if it knows the complete information about the other nodes. A sybil node can have any duplicate ID and duplicate information after obtaining this information. • A node can only communicate with other nodes after authorization by the network or from base station. According to authors, CAM is very effective and efficient as compare to other existing methods.
Energy and Hop based Detection	• The detection of malicious node is done in three phases, where in the first phase of method the node energies are compared with the threshold value. In the second phase the distance between suspected sybil nodes is calculated and finally, the route followed by the packets are checked for confirmation of a sybil node. • It is observed from the results that, the proposed scheme increase the Packet delivery ratio along with throughput of the network.
Threshold Elgamal Key Management Scheme	• To defend against the sybil attack proposed scheme validate each node identity to the only identity presented by the corresponding physical node, There are basically two ways to validate an identity. The first type is the direct validation in which a node directly tests another node identity. The second type is indirect one in which already verified nodes allowed to vouch for or refute other nodes. • In the proposed approach Elgamal based key management scheme is used. The Elgamal encryption scheme is an asymmetric key encryption algorithm used for public-key cryptography, which is based on the Diffie–Hellman key exchange. • A Threshold ElGamal-based key management scheme is used in this paper

	for protection against Sybil attack.
Optimized secure routing protocol	• The mechanism used in the paper is set up to detect sybil attack based on the distance and hop count between the nodes. • The prevention is done based on encryption technique which uses unique identities of the nodes. • The authors also calculate performance parameters energy consumption. The results show the efficiency of the proposed protocol. • The proposed work help in preventing the wireless sensor network from the security risk due to Sybil attack. The encryption technique used in the paper is based on the binomial distribution.
RSSI-based Scheme	• Authors present a robust and lightweight solution for sybil attack problem. The solution is based on received signal strength indicator (RSSI) which is used for readings of messages. • Authors claim that their solution is robust as it detects all sybil attack cases with less than a few percent false positives.
Channel-Based Detection	• An enhanced physical-layer authentication scheme to detect sybil attacks is proposed in. • This exploits the spatial variability of radio channels in the environments with rich scattering. Authors build a hypothesis test in order to detect sybil clients for both narrowband and wideband wireless systems, Based on existing channel estimations mechanisms, proposed method can be easily implemented with low overhead. This can be done either independently or combined with other physical-layer security methods. • The performance of proposed sybil detector in the paper is verified, via both a propagation modeling software. A field measurement using a vector network analyzer is also used for typical indoor environments. Authors claim that their evaluation examines numerous combinations of system parameters such as bandwidth, number of channel estimates, signal power, number of total clients, number of sybil clients, and number of the access points. According to authors, both the false alarm rate and the miss rate of sybil attacks are below 0.01, pilot power of 10 mW, with three tones, and a system bandwidth of 20 MHz..
	• This scheme proposes development of a defense scheme against direct, simultaneous sybil attacks with derivation of a rigorous analytic framework for the determination of the system performance. • This scheme focuses on a rule-based anomaly detection system. This system is called RADS, which monitors and timely detects Sybil attacks in large-

UWB ranging-based information	scale WSNs. The proposed expert system relies on an ultra-wideband (UWB) ranging-based detection algorithm. This algorithm usually operates in a distributed manner that require no information sharing or cooperation between the sensor nodes in order for performing the anomaly detection tasks. • In the paper feasibility of the proposed scheme is proven analytically. The performance of RADS in exposing sybil attacks is extensively assessed both numerically or mathematically. According to authors, the obtained results demonstrate that RADS achieves high detection accuracy along with low false alarm rate.

III. OTHER METHODOLOGIES

In the LEACH and LEACH-E (AlakeshBraman et al. 2014 [3]) protocols, the communication between cluster heads and the base station requires more energy than the non-cluster nodes. This means increasing the number of clusters-heads can increase the energy consumption of the whole network and shorten the network lifetime. Therefore, it is necessary to select the optimal number of cluster heads to make the energy consumption minimum. The original LEACH-E algorithm, selects the cluster heads at random with fixed round time for the selection. It considers the remnant power of the sensor nodes in order to balance network loads and changes the round time depending on the optimal cluster size. In LEACH-C (Shuo Shi et al. 2012;Petre-CosminHuruială et al. 2010; Raed M. Bani Hani and Abdalraheem A. Ijjeh. 2013 [20]) protocol, each node transmits its information to the corresponding base station and the sink node makes the choice of selecting the cluster head and how to divide clusters. Then the cluster head sends this information to BS. In Hierarchy routing protocol a CH collect a data from its cluster members, aggregates all data and forward to the BS that might be located far away from it. If the CH is compromised then it will be dropped. The compromised CH will become ineffective, because the data aggregated by cluster head will never reach the base station. V-LEACH (BaniYassein. M et al. 2009 [4]) protocol, besides having a CH in the cluster, also has a vice-CH that takes the role of the CH when the CH is dropped/compromised. The vice-cluster nodes forward data directly to the BS. Messy GAs solve (Goldberg . D et al.1989 [6]) problems of coverage of local maxima by the optimal search. To choose the best CH, minimizing the energy consumption and latency is obtained by choosing the best nodes in the network.

A genetic algorithm is executed on a central BS and the results are send to the nodes (Goldberg . D et al.1989 [6]). Hierarchical routing protocol (Vikram Mehta and Dr.Neena Gupta. 2012) due to a battery replacement or recharging is not realistic.

Choosing the routing protocol is, it must be energy-efficient to improve the network lifetime (Yang Yu et al. 2006;Manimozhi. B &, Santhi.B.2013 [10]). The optimal set of protocols is proposed to show the optimization in genetic algorithm metrics for WSNs with the QoS requirements (JiaXu,Ning et al. 2012 [16]). Cluster-based LEACH routing protocol in WSN has greater energy efficiency and the information such as node's residual energy and geometric distance send to BS, to elect CH nodes. The CH node is one hop to the BS to consume less energy than other nodes because communication of data consumes the more energy. CH nodes not only

consider the residual energy of the nodes and also distance between the CH and BS also examined (Jin Fan and Parish D .J. 2007 [6]). Trust-based LEACH protocol in (Nguyen Duy Tan et al. 2012 [12]) discussed the cluster-head-assisted monitoring control. Basic classification of routing protocols in WSNs (Petre-CosminHuruială et al. 2010 [21]) has named LEACH as the most energy efficient protocol giving its advantages and disadvantages. [19]

3.1 Leach-E Protocol

LEACH-E protocol improves the CH selection procedure. Sensor node's residual energy is the main concern, which decides whether the node become a CH or not after the first round (BaniYassein .M et al2009). Like LEACH protocol, LEACH-E is divided into rounds (Shankar .M et al. 2012). In the first round, all the nodes have the same probability of being a CH. At the end of the first round, the node, which has more residual energy, is elected as CH. LEACH–E protocol improves the cluster head selection procedure. [19]

3.2 Leach-E-GA (Leach-Energy-Genetic Algorithm)

This methodology uses the LEACH-Genetic algorithm (GA) that would enhance the WSN response time, network life and minimize the delay. The Genetic algorithm proposed by (Goldberg et al in 1975;Wu Xinhua and Wang Sheng. 2010) improves the cluster heads selection process. Selecting the minimum number of cluster heads in the WSN is determined based on the square root of the total number of sensor nodes, to minimize the total energy consumption.

The LEACH-E Genetic algorithm is shown in figure 3.1 selects an unsupervised node, which allows the network to achieve maximum coverage distance with minimum energy consumption. Genetic algorithm optimizes the behavior of the node based on its request and response, energy level, mobility and comparison with its record of previous transmissions.

A node, whose behavior is changed and not fit to the fitness function, is considered to be the Sybil node. The node is dropped from the network to improve the quality of the network for future communication.

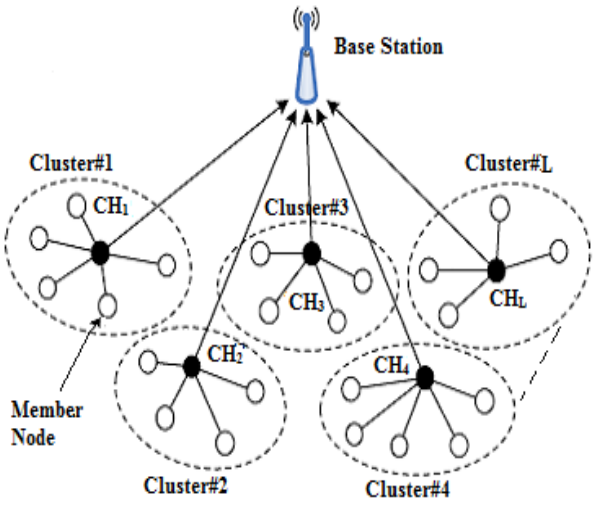

Figure 3.1 GA Hierarchical Clustering [19]

(Wu Xinhua & Wang Sheng. 2010) enhanced the HCR protocol using GA, which determines the clusters, CHs, Cluster-members and the schedules for transmission.

In this system, the GA can be used at any place in the network like base station CH, or in administration and it provides more energy efficiency by identifying the Sybil nodes to the optimizer. In each round of routing discovery, GA is applied. The optimizer chooses the best trusted neighbor nodes using the GA fitness function. The fitness function is based on the node behavior, direct distance to destination node, and energy and trust value of the nodes in the route. LEACH-E is enhanced by GA at the base station. GA creates the energy efficient clusters for more numbers of transmissions. In terms of GA representation, nodes are called [assigned] as chromosomes. The head node, member node in a cluster can be represented as a tuple < X, Y>.

A population contains a constant number of chromosomes, whereas the best chromosome can be used for next new population generation.

Genetic_Algorithm ( )

{

- Initialize population and Objective Function Value-[OFV].
- Define the Fitness function.
- Selection.
- Cross over.
- Mutation.
- Repeat the above steps until reaching the solution.

}

A population contains a group of individuals named chromosomes, which represents a finished solution for a derived problem. Each chromosome is a sequence of values of the attribute [node-energy, node-trust value, and node-distance].

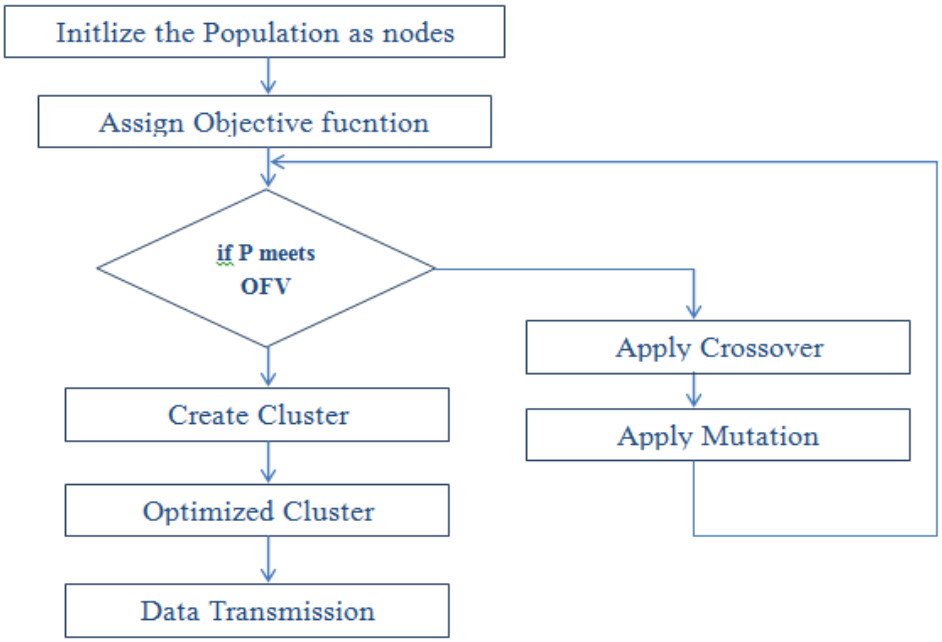

Figure 3.2 GA Flowchart used for WSN [19]

Once an initial population is randomly generated, the algorithm evolves through three operators:

1. Selection: This equates to survival of the fittest.
2. Crossover: This represents mating between individuals.
3. Mutation: This introduces random modifications.

1. Selection Operator

• Give preference to better individuals, allowing them to pass on their genes to the next generation.

• The goodness of each individual depends on its fitness.

• Fitness may be determined by an objective function or by a subjective judgment.

2. Crossover Operator

Crossover is a significant operator of the GA.

The primary aim of crossover is to reorganize the information of two different individuals and create a new one. It is a structured, yet randomized method of exchanging formation between strings. It encourages the exploration of new fields in search space. Cross swapping operator is used on the chosen individuals.

Here, two different cross sites of parent chromosomes are selected randomly. The cross over operation is finished by exchanging the middle substring between strings.

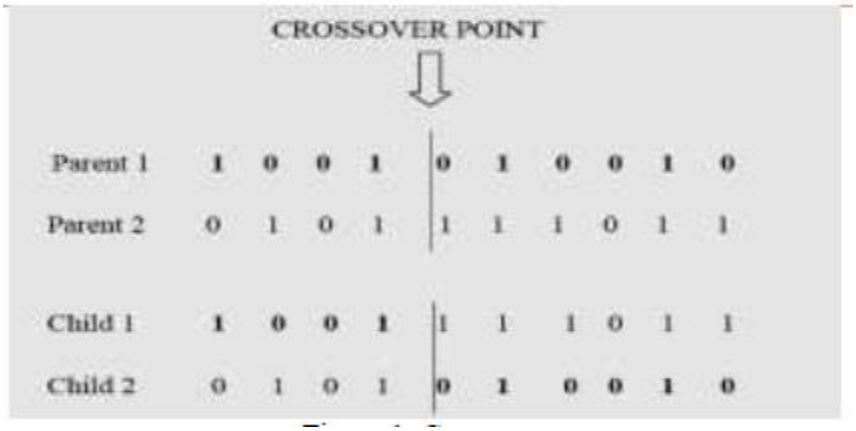

Figure 3.3 Crossover [20]

3.Mutation Operator

Mutation consists of securing the procedure of reproduction and crossover efficiently without much loss of the potentially helpful genetic material. Mutation is by itself a random walk through the string space and offers for occasional interference in the crossover operation by introducing one or more genetic elements during reproduction. This operation assures diversity in the genetic strings over large period of time and prevents stagnation in the emergence of optimal individuals. Bit wise mutation changes 1 to 0 and vice-versa. The above specified operations of selection, crossover and mutation are repeated until the best individual is detected.

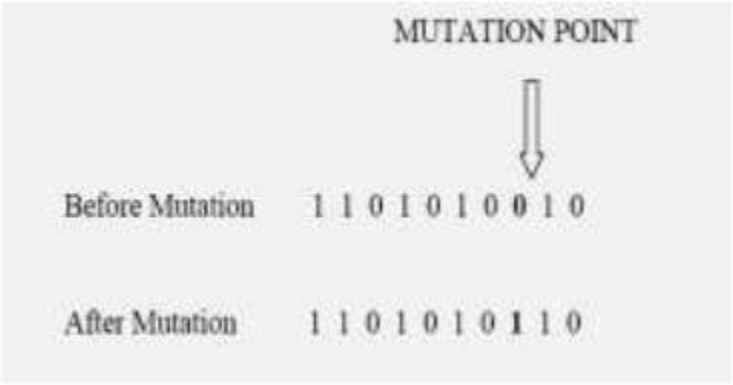

Figure 3.4 Mutation [20]

IV. CONCLUSION

The applications of wireless sensor network are increasing along with the need for more effective security mechanisms.

The security concerns of the WSNs should be addressed from the beginning of designing of the system, since sensor networks interact with sensitive data and they usually operate in hostile

unattended environments. A thorough understanding of the capabilities and limitations of each of underlying technology is required for the secure working of wireless sensor networks. In Sybil attack, a node illegitimately claims multiple identities or claims fake IDs in order to collapse the sensor network. A thorough study of limitations of available techniques will help in the design of novel, robust, and secure mechanism against Sybil attack, so that the sensor network applications can be extended to other fields.

The aim of the cluster based Hierarchy routing protocol LEACH-E (Low Energy Adaptive Clustering Hierarchy-Energy) is to provide secure routing and to preserve the functionalities of the original protocol. This energy efficient protocol always elects a Cluster Head (CH) based on high energy among the cluster group. Here we propose a LEACH-E-GA for Intrusion detection (ID) in Wireless Sensor Nodes. The Genetic Algorithm is deployed into LEACH-E to provide prevention for Sybil attacks. The objective of this Genetic Algorithm (GA) is to identify its best trusted neighbors for communication using its optimization capability. LEACH-E-GA reduces an inside Sybil attack in WSN and shows reliable transmission with improved network efficiency, reduced delay and increased packet delivery ratio.

In LEACH-E-GA algorithm the node behavior is controlled and network prolong lifetime is improved. With this algorithm we can extend the work to monitor the network using Intrusion Detection Protocol using Cryptography.

4.1 Future work

In future work new issues and new methodologies could be included related to increasing complexity and increasing detection time for Sybil node when more number of nodes present in the networks.

In wireless sensor networks, the energy limitations of nodes play a crucial role in designing any protocol for implementation. The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide

security, one is cryptography. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches.

REFERENCE

[1] A. Babu Karuppiah and A. Raja Prakash, "SYBILSECURE: an energy efficient sybil attack detection technique in wireless sensor network," International Journal of Information Sciences and Techniques (IJIST) Vol. 4, No. 3, May 2014.

[2] A. V. Vibi, G. V. Padmasree, P. Nithya, and C. Geetha, "Detection of sybil attack using neighboring node messanging using wireless sensor network," International Journal of Advanced Technology in Engineering and Science, Volume No. 3, Issue No. 3, March 2015, ISSN (online): 2348 – 7550.

[3] Alakesh, B., & Umapathi, G. R. (2014). A Comparative Study on Advances in LEACH Routing Protocol for

Wireless Sensor Networks. A survey International Journal of Advanced Research in Computer and Communication Engineering, 3(2).

[4] Bani, Y. M. et al. (2009). Improvement on LEACH Protocol of Wireless Sensor Network (VLEACH). International Journal of Digital Content Technology and its Applications, 3(2).

[5] Dr. Shu Yinbiao, Dr. Kang Lee, Mr. Peter Lanctot," Internet of Things: Wireless Sensor Network " White Paper 2014 International Electrotechnical Commission-IEC, China (http://www.iec.ch).

[6] Goldberg, D. et al. (1989). Messy genetic algorithms: Motivation, analysis, and first results. The Clearing

[7] house for Genetic Algorithms (TCGA), Report 89003.

[8] John R. Douceur, The attack, (2002), 251–260. http://shodhganga.inflibnet.ac.in/bitstream/10603/22912/7/07_chapter_01.pdf

[9] Manju V C, Research Scholar, Kerala University, Research Centre LBS Center, Kerala, India," SYBIL ATTACK PREVENTION IN WIRELESS SENSOR NETWORK", International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC) Vol. 4, Issue 2, Apr

[10] 2014, 125-132.

Manimozhi, B., & Santhi, B. (2013). Comparison of Different Performance Measures of Routing protocols in WSN. International Journal of Engineering and Technology (IJET),5, 208-214.

[11] Ms. Reena S. Satpute, Prof. R. S. Mangrulkar,and Prof. A. N. Thakare" Performance Analysis of Wireless

Sensor Networks using Elliptical Curves Cryptography" B.D.C.O.E., Sevagram Maharashtra, India- Pin Code-442001. International Journal of Engineering Research & Technology (IJERT) Vol. 3 Iss7,

[12] July - 2014 ISSN: 2278-0181

Nguyen, D. T. et al. (2012). An Improved LEACH Routing Protocol for Energy-Efficiency of Wireless

[13] Sensor.

Ning, J. X. et al. (2012). Improvement of LEACH protocol for WSN. 9th International conference on

Fuzzy
Systems and Knowledge Discovery.

[14] P. R. Gundalwar, Dr. V. N. Chavan," A literature review on Wireless Sensor Networks (WSNs) and its Diversified Applications" International Journal of Advanced Research in Computer Science (IJARCS 2012), Volume 3, No. 7, Nov-Dec 2012 ISSN No. 0976-5697

[15] Panagiotis Sarigiannidis, Eirini Karapistoli and Anastasios A. Economides, "Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information," Expert Systems with Applications: An International Journal, Volume 42, Issue 21, November 2015.

Petre-Cosmin, H. et al. (2010). Hierarchical Routing Protocol based on Evolutionary Algorithms for Wireless Sensor Networks. 9th RoEduNet IEEE International Conference 2010.

[17] Prabhjotkaur, Aayushi Chada, Sandeep Singh," Review Paper of Detection and Prevention of Sybil Attack in WSN Using Centralizedids", International Journal of Engineering Science and Computing (IJESC), July 2016, Volume 6 Issue No. 7

[18] R. Amuthavalli and R. S. Bhuvaneswaran , " Detection and Prevention of Sybil attack in Wireless Sensor Network Employing Random Password Comparison Method," Journal of Theoretical and Applied Information Technology, September 2014, Vol. 67, No.1, ISSN: 1992- 8645.

[19] R. Amuthavalli & R. S. Bhuvaneswaran, "Genetic Algorithm Enabled Prevention of Sybil Attacks for LEACH-E", in Modern Applied Science Vol. 9, No. 9; 2015, Published by Canadian Center of Science and Education.

[20] Raed, M. B. H., &Abdalraheem, A. I. (2013). A Survey on LEACH-Based Energy Aware Protocols for Wireless Sensor Networks. Journal of Communications, 8(3).

[21] Reza Rafeh and Mozhgan Khodadadi , " Detecting Sybil Nodes in Wireless Sensor Networks using Two- hop Messages," Indian Journal of Science and Technology, Vol. 7(9), 1359– 1368, September 2014, ISSN (Print) : 0974- 6846 ISSN (Online) : 0974-5645.

[22] Rupinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh," SYBIL ATTACK COUNTERMEASURES
IN WIRELESS SENSOR NETWORKS", International Journal of Computer Networks and Wireless Communication, Vol.6, No 3, May-June 2016, ISSN: 2250-3501(IJCNWC 2016)

[23] S. Sharmila and G. Umamaeshwari, " Energy and Hop based Detection of Sybil attack for Mobile Wireless Sensor Networks," International Journal of Emerging Technology and Advanced Engineering, Volume 4, Special Issue 4, February 2014, ISSN 2250-2459.

[24] Seyit A. Camtepe and B¨ulent Yener, "Key distribution mechanisms for wireless sensor networks: a Survey".

[25] Sunil Ghildiyal, Ashish Gupta, Nitesh Tomar, Anupam Semwal," Analysis of Sybil Attack in Wireless Sensor Networks" International Journal of Engineering Research & Technology (IJERT 2014) Vol. 3

Issue 5, May – 2014, ISSN: 2278-0181. www.ijert.org

[26] Sweety Saxena and Prof. Vikas Sejwar, " Sybil Attack Detection and Analysis of Energy Consumption in Cluster Based Sensor Networks," International Journal of Grid Distribution Computing Vol. 7, No. 5 (2014), pp.15-30, ISSN: 2005-4262.

[27] Tanya Roosta, S. P. Shieh, and Shankar Sastry," Taxonomy of security attacks in sensor networks and Countermeasures", The First IEEE International Conference on System Integration and Reliability Improvements, December 2006."

[28] Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE journal on selected areas in communications, Vol. 29, No. 3, March 2011.

[29] Udaya Suriya Rajkumar and Rajamani Vayanaperumal, "Compare and Match Approach for Preventing Sybil Attacks in Wireless Sensor Networks," International Journal of Engineering Technology Science and Research, Volume 2, Special Issue September 2015, ISSN 2394 –3386.

[30] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method," Scientific World Journal, 2015.

[31] V. Sujatha and E. A. Mary Anita, "Detection of Sybil Attack in Wireless Sensor Network," Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 202-206, 2015, ISSN 1990-9233.