International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

A REVIEW ON SYBIL ATTACK IN WSN

Inderpreet singh[1], Rajan kumar[2]

[1]*PG Student ,Chandigarh University ,Punjab, India*
[2]*Assistant Professor, Chandigarh University ,Punjab, India*

Abstract: *In recent development with distribution of wireless sensor network ,wireless communication and growing trendness of mobile devices create it popular area of interest from research point of view. Due to decentralized nature of wireless sensor networks, the malicious nodes join the network which is responsible to trigger various types of attacks. The Sybil attack is one of these attacks which is very dangerous attack against sensor grid. In this paper, A survey is done on various detection techniques of Sybil attack is described.*

Introduction:

Wireless sensor network is a network in which various number of connections like sensor nodes are linked together to communicate with one another in order to form a network known as WSN network. For the secure communication between two devices a strong network is generated. All the communications in the wireless network performed over the wireless medium. There are different applications in demand of communications networks such as ad-hoc networks, mesh network etc. The communication environment in the wireless network is the radio frequencies, infrared or other wireless media. In order to perform functions various numbers of computers are connected together in which there are not connected through wires. An ad-hoc network can be generated using sensor nodes randomly so that they can communicate with each other. The combination of all networks form shared resources that can be software or hardware. This is used widely in the research theme as they have many advantages like economic potential, capacity to transform lives or easy the life etc. Sensor nodes in the wireless network provide the information of surroundings as they monitored the different conditions at different locations. They can sense the humidity, pressure, soil, noise and temperature. A sensor is very important to exchange information between the networks.

Literature Review:

Imran Makhdoom, et.al (2014) presented that there are various types of internal as well as external attacks possible within the wireless sensor networks due to their distributed nature. The external attacks are prevented from entering the network with the help of classic cryptographic measures up to some level. However, the internal attacks cannot be detected in proper manner with the help of these methods. In order to introduce the Sybil attack in the network, there is a compromised node is placed in the network. a detailed review of the proposed techniques is presented in this paper and the techniques are analyzed in terms of several parameters. The advantages and disadvantages of all these techniques are highlighted on the basis of various platforms. A novel technique known as One Way Code Attestation Protocol (OWCAP) is also presented in this paper that provides a secure code attestation method which helps in protecting the network against the Sybil attack.

Bayrem Triki, et.al (2014) proposed a novel technique to identify and prevent Sybil attacks from the Military Wireless Sensor networks (MWSNs). There are two types of authentication methods provided to identify the Sybil attacker from the network. In the initial type, the RFID tags are utilized that are embedded within the soldiers in order to provide authentications to them along with the certificates. Further, these certificates are utilized by the soldiers. This helps in providing an authentication of the soldiers to their respective neighbors available. The soldiers that use two valid certificates at similar time can be recognized which can help in recognizing the Sybil attacks present in the networks. In order to enforce authentication to the soldiers, their heartbeat is used. The team leaders of the soldiers also utilize such private information in order to recognize the Sybil attacks present in the systems.

Noor Alsaedi, et.al (2015) presented that within numerous applications, wireless sensor networks have been deployed which monitor the surrounding areas. Due to small processing power as well as the wireless communication provided in the networks, the sensing capabilities are combined due to which the sensor networks perform more efficiently. There are large numbers of attacks possible which can deplete the security of these networks even though they have highly attractive properties. The security related issues become more complex when the properties such as limited energy and memory exist within these networks. The Sybil attacks are also possible within the WSNs. The network can be disrupted here due to the presence of adversary that forges the number entities help of energy parameters within these networks. A novel trust system is deployed in

this paper with the various experiments are conducted in the networks which identify the Sybil attack from which the results are achieved which show that the proposed technique is highly efficient and scalable. The communication overhead is also minimized within the network due to the application of this technology is the wireless sensor networks.

Salavat Marian, et.al, (2015) presented that there are several attacks that are possible within the wireless sensor networks amongst which the Sybil attack is the most commonly found attack. A false identity of other nodes is assumed by the Sybil node from the network. Multiple IDs of the nodes are generated by broadcasting various packets in the network which creates a great fuss within the networks. There are further many attacks generated within the network after Sybil attack gets introduced in the network. A robust and simple solution is provided in this paper in order to prevent Sybil attack from entering the network. The received signal strength indicator (RSSI) technique is used as base in order to propose the new technique. In order to provide link quality estimation, there are two known indicators that are utilized within these networks. They are Received Signal Strength Indicator and Link Quality Indicator (LQI). Through various experiments that are conducted using proposed algorithm it is seen that when this system is applied in static environments, the performance of this algorithm is very efficient with respect to various aspects.

Sepide Moradi, et.al (2016) presented that there is an increase in demand of wireless sensor networks with time. In order to gather the data within various distributed scenarios, the sensor nodes are available within the networks. There is a need to secure the wireless scenarios as these environments are not secure. In order to ensure the security of these environments, there is a need to identify the attacks that are present within the WSNs. Amongst all the attacks possible, there is Sybil attack which is possible within these networks. In order to degrade the performance of geographical routing protocols along with multi-path routing, various attacks are generated purposely or by chance within the networks. By utilizing mobile agents along with the local information of each of the sensor that identifies the Sybil attack, a distributed technique is proposed in this paper. The comparison is presented in this paper in order to evaluate the efficiency of the method given by author in this paper. Author concluded that their experimented method is better than the existing methods.

Panagiotis Sarigiannidis, et.al (2016) have presented in this paper the importance of wireless sensor networks today's. In order to gather the data within various distributed scenarios, the sensor nodes are available within the networks. There is a need to secure the wireless scenarios as these environments are not secure. For the area monitoring sensor nodes are deployed when it is required to monitor the physical activity. When any activity is sensed by sensor nodes like any noise, vibration a report of detection send to the base station. After sending information to the base station appropriate action is taken by it. The areas where sensor nodes are used to identify any distortion this area is known as sensor areas. Due to the presence of open wireless networks huge number of serious attacks occurred in the network. This happens due to open wireless networks sensor nodes start communicating with each other and to the external network also. The attack in which one malicious node generates numerous identities is known as a Sybil attack. Due to the various characteristics of wireless sensor networks, this attack is highly vulnerable to these networks. They also result in generating a gateway to all the other various attacks. Within the peer to peer networks, the Sybil attack was introduced which caused the generation of various issues within the network. Author in this paper presented that efficient and effective results can be achieved using this proposed technique.

Sybil Attack : The attack in which one malicious node generates numerous identities is known as a Sybil attack. Due to the various characteristics of wireless sensor networks, this attack is highly vulnerable to these networks. They also result in generating a gateway to all the other various attacks. Within the peer to peer networks, the Sybil attack was introduced which caused the generation of various issues within the network The issues arising here mainly are related to distributed storage, voting, resource allocation and various such operations going on within these networks. However, the traditional security related techniques could not ensure that all such problems could be avoided as they had the limited sensor nodes present in them. Thus, there is a need to make enhancements within this method yet. A general Sybil attack scenario is explained below.

Creation of Sybil nodes in sensor network: Depending on the communication, spontaneity, as well as the identities of the network, the Sybil attack can be generated in different forms. During the communication of one hop communication on the node, the nodes communicate with each other as per this scenario. The access to normal nodes is gained by such types of compromised node. The general information can be extracted very easily from the normal node by the malicious nodes. Similar identities can be generated by the attacker with the help of this knowledge. This results in causing a scenario through which the normal nodes are attacked further. This generated great confusion within the network and corrupts them.

i. **Direct and indirect communication**: The attacker generates the Sybil node within the direct communication through which the attacker communicated to the normal nodes. The malicious nodes are used to communicate directly with the normal node within the indirect communication.

ii. **Stolen and Fabricated identities**: New absolute identities are generated by the attacker by fabricating the identities of normal nodes. The malicious node steals identifies from the legitimate node. Similar to the stolen identities, the new identities are generated by the malicious node.

iii. **Simultaneous and non simultaneous:** The numerous identities are generated by the attacker that is present within the network at the similar duration of time as those of other nodes which is known as simultaneous nodes. The multiple identities can be present within the participating nodes that occur individually within the non-simultaneous attacks.

Techniques for Isolation of Sybil attack:

1. Mobile Agents technique: - In this technique by utilizing mobile agents along with the local information of each of the sensor that identifies the Sybil attack. This technique detects the maximum malicious nodes in the least amount of time.

2. Monitor Mode technique: - In this technique, each node start watching its adjacent node. The node which spoofs credentials of the base station will be detected as the malicious node.

3. Trust based technique:- A novel trust system is deployed in this paper with the help of energy parameters within these networks. Various experiments are conducted in the networks which identify the Sybil attack from which the results are achieved which show that the proposed technique is highly efficient and scalable.

4. Cryptographic Technique: - The external attacks are prevented from entering the network with the help of classic cryptographic measures up to some level. However, the internal attacks cannot be detected in proper manner with the help of these methods. In order to introduce the Sybil attack in the network, there is a compromised node is placed in the network. a detailed review of the proposed technique.

Conclusion:

In this work, it is been concluded that LEACH protocol is the most efficient protocol to reduce energy consumption of wireless sensor network. The networks that can sense the environmental conditions with the help of sensor nodes present within them are known as wireless sensor networks. The sensed information is gathered and passed further to the base station. The sensor nodes are of very small size. Therefore, the lifetime of the sensor nodes is very less and the size of battery available within them is very less. The sybil attack is the active type of attack which reduces performance of LEACH protocol.

References:

[1] Imran Makhdoom, Mehreen Afzal, Imran Rashid, "A Novel Code Attestation Scheme Against Sybil Attack in Wireless Sensor Networks", 2014 National Software Engineering Conference.

[2] Noor Alsaedi, Fazirulhisyam Hashim, A. Sali, "Energy Trust System for Detecting Sybil Attack in Clustered Wireless Sensor Networks", 2015 IEEE 12th Malaysia International Conference on Communications (MICC).

[3] Bayrem Triki, Slim Rekhist, Noureddine Boudrigat, "An RFID based System for the detection of Sybil attack in Military Wireless Sensor networks", 2014, IEEE .

[4] Salavat Marian, Popa Mircea, "Sybil Attack Type Detection in Wireless Sensor Networks based on Received Signal Strength Indicator detection scheme", 2015, 10th Jubilee IEEE International Symposium on Applied Computational Intelligence and Informatics.

[5] Sepide Moradi, Meysam Alavi, "A distributed method based on mobile agent to detect Sybil attacks in wireless sensor networks", 2016 Eighth International Conference on Information and Knowledge Technology (IKT).

[6] Panagiotis Sarigiannidis, Eirini Karapistoli and Anastasios A. Economides, "Analysing Indirect Sybil Attacks in Randomly Deployed Wireless Sensor Networks", 2016 IEEE 27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communication.

[7] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter," An experimental study of selective cooperative relaying in industrial wireless sensor networks," IEEE Trans. Industrial Informatics, vol. 10, no. 3, pp. 1806-1816, Aug. 2014.