International Journal of Future Generation Communication and Networking
Vol. 13, No. 4, (2020), pp. 890 – 895

Review of Various Technique for the Isolation of sinkhole attack from WSN

Sumedha

(ssumedha809@gmail.com),

Dr Nagesh kumar

(Nageshkumar@shooliniuniversity.com)

Shoolini university,solan

Abstract

The wireless sensor network is the decentralized type of network in which sensor nodes can join or leave the network when they want. Due to such type of network many malicious nodes can join the network which triggers various types of active and passive attacks. The sink hole attack is the active type of attack which reduce network performance in terms of certain parameters. The various techniques are designed which can detect and isolate malicious nodes from the network. In this paper, sinkhole isolation and detection techniques are reviewed in terms of certain parameters

Keywords

WSN, Sinkhole, Active attack, Watchdog

Introduction

WSN (Wireless Sensor Network) can be described as a self-organized and infrastructure less wireless network of sensor nodes. These sensor nodes perform the monitoring of physical or environmental conditions such as humidity, sound, vibration etc. The sensor nodes collectively forward their data via the network to a base station or sink. At base station, the observing and analysis of data can be done [1]. A sink or base station acts as a link between users and the network. It is possible to extract necessary information from the network by inserting queries and collecting outcomes from the base station. In general, a wireless sensor network consists of several hundreds or thousands of sensor nodes. The sensor nodes can establish communication with each other through radio signals [2]. A deployment of wireless sensor node is carried out with sensing and computing devices, radio transceivers and energy elements. In WSN (wireless sensor network), the individual nodes intrinsically have limited resources. These nodes have restricted processing speed, storage ability, and transmission bandwidth. The deployed sensor nodes are accountable for the self-configuring of a suitable network framework [3]. The sensor nodes generally communicate with each other through multi-hop communication. After the configuration of network, the deployed sensors begin to gather required information. The queries transmitted from a “control site” are also responded by sensor nodes for performing particular tasks or providing sensing patterns. The sensor nodes may work either in continuous way or as per the event. It is possible to outfit wireless sensor nodes with actuators to “act” in certain situations [4]. Occasionally, these networks are termed as Wireless Sensor and Actuator Networks. The concerns related to security in a sensor network rely on type of object which needs security. There are mainly four objectives in sensor networks. These objectives are identified as confidentiality, integrity, authentication and availability. The potential to hide information from a passive intruder, where the information transmitted on sensor networks keeps secret is called confidentiality. The potential of confirming the non-tampering, non-altering and unchanging of information during its occurrence on the network is called integrity [5]. Authentication confirms the location of messages from the same node where it is being claimed. This aim determines the trustworthiness of message's source. Availability can be described as the node's potential of using the resources. This objective ensures the availability of the network for the forwarding of messages. Originality means that that receiver gets the current and new data. Originality makes certain that opponent cannot replay the previous data. This prerequisite is particularly significant when the WSN devices make usage of shared-keys for transferring information [6]. In such situation, an able opponent may trigger a replay attack by replacing old key with the new key and propagating these keys to all the nodes within the network. The scheme such as nonce or time stamp should be added to every data packet for achieving originality. There are basically two major categories of intrusions or attacks as per the disruption in message transmission. These attacks are classified as passive attacks and active attacks. In Passive Attacks the adversary listens and scrutinizes the shared traffic [7]. These sorts of intrusions can be launched easily merely using a satisfactory receiver. However, the detection of these attacks is quite hard. In Active attacks, an intruder makes an attempt for removing or modifying the messages delivered on the network. The attacker may also insert his own traffic or can replay previous messages for causing disruption in the functioning of the network. In WSN (wireless sensor networks), an individual node, called a faulty device may create numerous IDs (identities) for getting the illegitimate access of the network. The main purpose here is to trick the genuine nodes using these generated identities as multiple nodes. In such a situation, the penetration in the network can be done for launching an attack. The multiple nodes generated by malevolent node are known as Sybil nodes [8]. The successfulness of this kind of intrusion is known as Sybil intrusion or Sybil attack. This attack is recognized as serious threat in the sensor network's architecture. The attack can be mitigated in wireless sensor network for stationary nodes. However, the sensor network that mitigates mobile Sybil nodes are not designed yet. Figure 1 show a general Sybil attack event where an intruder is masked as different nodes.

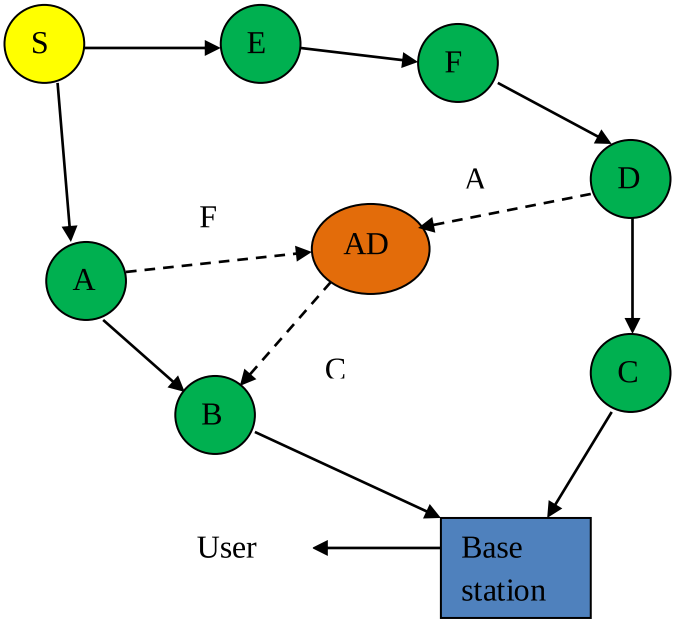

Figure 1: Sybil Attack

As shown in figure 1, multiple identities are shown by an adversary node 'AD'. Node 'F' appears for 'A', node 'A' for 'D' and node 'C' for 'B' for node 'AD'. So, the message is forwarded to 'AD' when node 'B' wants to communication with node 'C'. The Sybil attack can cause disturbance in the normal functioning of network.

Literature Review

Shehnaz T. Patel, et.al (2017) described WSN (Wireless Sensor Network) as a network of tiny sensor nodes [9]. The nodes within this network established communication with each other through wireless link. Monitoring ecological conditions was the main aim of these tiny sensor nodes. These networks were generally used in various applications particularly for army and civil purposes. The deployment of these networks was done in the distant locations. The networks in such locations were vulnerable to different types of security intrusions. Studying, discussing and analyzing the different Sybil intrusion detection approaches in WSN was the main aim of this work. Moreover, this work considered and examined several protocols attacked by Sybil intrusion.

Noor Alsaedi, et.al (2015) stated that wireless sensor networks were prone to different types of security intrusions [10]. This network had several issues such as less energy, low memory etc. All these issues made security within this network more challenging. A lightweight trust system was developed in this study to deal with this issue. This system used energy as a performance metric for a hierarchical WSN (Wireless Sensor Network). The efficiency and scalability of this system in the detection of Sybil attack was demonstrated by evaluating the performance of this system in terms of true and false positive rate in a dynamic WSN (wireless sensor network). In addition, this system cancelled feedback and suggestions amid sensor nodes for reducing the cost of information sharing.

Yali Yuan, et.al (2018) recommended a secure APIT Localization approach against Sybil intrusions in dispersed WSNs (Wireless Sensor Networks) [11]. It was an efficient range-free technique. This approach was implemented at a single node in a completely distributed way. The recommended approach required less costly wireless devices. This approach showed good performance in terms of received signal power. The simulations results depicted that this approach efficiently detected Sybil intrusions and defended wireless sensor network against these intrusions. This approach achieved high detection rate in spread wireless localization designs.

Surinder Singh, et.al (2018) stated that WSN (wireless sensor network) was made up of various important components [12]. A sensor node had the ability to compute various non-electrical parameters. The sensor nodes made use of trans-receiver for transmitting the collected information to the sink node. It was essential to provide security to this transferred data due to the probability of important information within the data. These networks were generally used for the army and civilian applications. This attack could severely influence the routing protocols, sensible resource distribution, data aggregation and misconduct detection metrics of the network. Among all recommended approaches merely few approaches could made improvement in the true recognition rate and decreased false recognition rate.

Sepide Moradi, et.al (2016) stated that the growth in the popularity of WSN (Wireless sensor network) was noticed with the time [13]. In these networks, detection of intrusions was essential for ensuring the security. These networks were prone to different types of security intrusions. One of such attacks was known as Sybil intrusion. This intrusion could be a huge danger to both geographical routing protocols as well as multipath routing protocols. In this work, a distributed technique was recommended for Sybil intrusion detection. The recommended technique used mobile agents and local data of all sensor nodes. The achieved simulation results demonstrated the efficiency of recommended approach in contrast to other existing approaches.

Salavat Marian, et.al (2015) recommended a new approach for detecting Sybil attack in wireless sensor network [14]. The recommended approach was quite robust and lightweight. This approach was based received signal strength indicator (RSSI). The contemporary WSNs (wireless sensor networks) had two identified indicators for estimating the quality of connection. These indicators were called Received Signal Strength Indicator and Link Quality Indicator (LQI). The tested results depicted that the first indication showed good stability in stationary situations and with efficient trans-receivers. The wireless channel models generally considered received power as a function of distance. However, this work used this function for the localization of Sybil nodes.

Qing Tang, et.al (2017) recommended a safe positioning algorithm against Sybil attack in wireless sensor networks [15]. The recommended approach was based on number allocation and the common guarantee of adjoining nodes. The neighboring nodes could deny the entry of a node within the network in case of incomplete matching of the declaration number, the guaranteed node and individual identity of a node. This approach also adopted the verification method of one-way hash function. The recommended approach did not require sink or cluster heads. As a result of this, the recommended approach received quick, frivolous and high recognition rate and hence secured localization. In contrast to other existing approaches, this recommended approach achieved better detection rate and positioning accuracy with less communication overhead.

Table 1: Table of Comparison

Authors Names	**Year of Publication**	**Description**	**Outcomes**
Shehnaz T. Patel, Nital H. Mistry	2017	The nodes within this network established communication with each other through wireless link. Monitoring ecological conditions was the main aim of these tiny sensor nodes.	This work considered and examined several protocols attacked by Sybil intrusion.
Noor Alsaedi, Fazirulhisyam Hashim, A. Sali	2015	A lightweight trust system was developed in this study to deal with this issue. This system used energy as a performance metric for a hierarchical WSN (Wireless Sensor Network).	The efficiency and scalability of this system in the detection of Sybil attack was demonstrated by evaluating the performance of this system in terms of true and false positive rate in a dynamic WSN.
Yali Yuan, Liuwei Huo, Zhixiao Wang, Dieter Hogrefe	2018	A secure APIT Localization approach was proposed against Sybil intrusions in dispersed WSNs (Wireless Sensor Networks).	This approach achieved high detection rate in spread wireless localization designs.
Surinder Singh, Hardeep Singh Saini	2018	A sensor node had the ability to compute various non-electrical parameters. The sensor nodes made use of trans-receiver for transmitting the collected information to the sink node.	Among all recommended approaches merely few approaches could made improvement in the true recognition rate and decreased false recognition rate.
Sepide Moradi, Meysam Alavi	2016	In this work, a distributed technique was recommended for Sybil intrusion detection. The recommended technique used mobile agents and local data of all sensor nodes.	The achieved simulation results demonstrated the efficiency of recommended approach in contrast to other existing approaches.
Salavat Marian, Popa Mircea	2015	A new approach was proposed for detecting Sybil attack in wireless sensor network.	The tested results depicted that the first indication showed good stability in stationary situations and with efficient trans-receivers.
Qing Tang,	2017	The neighboring nodes could deny the	In contrast to other existing

Jian Wang		entry of a node within the network in case of incomplete matching of the declaration number, the guaranteed node and individual identity of a node.	approaches, this recommended approach achieved better detection rate and positioning accuracy with less communication overhead.

Conclusion

In this paper, it is concluded that sink hole attack is the active type of attack which is possible in wireless sensor network. The sink hole attack is possible in the network due to decentralized nature of the network. The various techniques which are designed to isolate sinkhole attack in the network. The watchdog technique is the most efficient technique which can isolate malicious nodes from the network. In future, novel methodology will be proposed for the isolation of sinkhole attack from the network.

References

[1] Panagiotis Sarigiannidis, Eirini Karapistoli, Anastasios A. Economides, “Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information”, 2015, Expert Systems with Applications, Volume 42, Issue 21, , Pages 7560-7572

[2] Mojtaba Jamshidi, Ehsan Zangeneh, Mehdi Esnaashari, Mohammad Reza Meybodi, “A lightweight algorithm for detecting mobile Sybil nodes in mobile wireless sensor networks”, Computers & Electrical Engineering, Volume 64, November 2017, Pages 220-232

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

[4] 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).

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

[6] 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.

[7] 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).

[8] 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.

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

[10] 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)

[11] Yali Yuan, Liuwei Huo, Zhixiao Wang, Dieter Hogrefe, "Secure APIT Localization Scheme against Sybil Attacks in Distributed Wireless Sensor Networks", 2018, IEEE Access, Volume: 6

[12] Surinder Singh, Hardeep Singh Saini, "Security approaches for data aggregation in Wireless Sensor Networks against Sybil Attack", 2018, Second International Conference on Inventive Communication and Computational Technologies (ICICCT)

[13] 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)

[14] Salavat Marian, Popa Mircea, "Sybil attack type detection in Wireless Sensor networks based on received signal strength indicator detection scheme", 2015, IEEE 10th Jubilee International Symposium on Applied Computational Intelligence and Informatics

[15] Qing Tang, Jian Wang, "A secure positioning algorithm against Sybil attack in wireless sensor networks based on number allocating", 2017, IEEE 17th International Conference on Communication Technology (ICCT)