International Journal of Engineering & Technology, 7 (2.27) (2018) 118-121

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Mutual authentication technique for detection of malicious nodes in wireless sensor networks

Inderpreet Singh [1] *, Rajan Kumar [2]

[1] PG Student ,Chandigarh University ,Punjab, India
[2] Assistant Professor, Chandigarh University ,Punjab, India
**Corresponding author E-mail: Inderpreeet409@gmail.com*

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 self configuring nature of network security and energy, consumption is the major issue of the network. The Sybil is the denial of service type of attack in which sensor nodes can change its identification multiple times in the network. In this research work, mutual authentication technique is proposed which detect malicious nodes from the network which is responsible to trigger Sybil attack in the network. The simulation of proposed algorithm is performed in NS2 and results shows that proposed technique performs well in terms of energy and throughput

Keywords: *WSN; LEACH; Sybil; NS2*

1. Introduction

A group of distributed sensors which are responsible to monitor as well as record the information from surrounding areas and then transmit the data to central authority is known as wireless sensor network (WSN). The conditions such as temperature, pressure, levels of pollution, speed as well as direction of wind and so on are known through the information collected by the sensors. As per the application in which the network is being deployed, there are around hundreds to thousands of sensor nodes deployed in the regions. There are several components of a sensor node which include radio transceiver along with an antenna, an electronic circuit, a microcontroller, as well as a battery or any energy source. As per the functionality parameters included within a sensor, there is difference in their costs as well. The types of distributive networks that include similarities with typical computer network along with some unique constraints as per requirements are known as sensor networks. Thus, in order to ensure security within these networks, both of these requirements need to be taken care of. Attributes like confidentiality, integrity, availability as well as authentication are included within the basic security requirements of WSN. In order to prevent the networks from being vulnerable to different attacks these properties need to be ensured. The sensor networks are vulnerable to security threats mainly because of the unique properties of the available networking protocols [1]. The WSNs have different layers in their architecture and the attacks can occur at any of these layers which are namely physical layer, link layer, network layer, transport layer as well as application layer. Not all the routing protocols have the motive of providing security to the networks. Due to this reason, the networks are highly prone to different types of attacks. There are several layer wise attacks studied by various researchers. Jamming and Tampering are two of the attacks found in physical layer. The attack that targets the availability of the network and causes interference in the radio frequencies of the devices of network is known as jamming attack. Denial-of –service type of attack can be caused due to the unwanted and disruptive scenario is generates. The attack in which a node is captured of compromised within the network is known as tampering attack. The possibility of this attack to occur is very high and its preventive measures available yet are very less [2], [13], and [14]. The sensor nodes are physically modified and destroyed due to this attack. Collision and exhaustion are two types of attacks found in the link layer. A type of link layer attack in which the neighbor to neighbor communication being held at the channel arbitration is controlled is known as collision. Even if in a part of the transmission some collisions are generated by come compromised node, the entire packet can be disrupted. Through the single bit error, there might be a chance to provide retransmission here. An interrogation attack which is generated when a battery power of a network is exhausted is known as exhaustion. Higher consumption of battery can be caused when a compromised node makes transmissions repeatedly here. Hello flood attack, wormhole attack, Sybil attack and sinkhole attack are few of the attacks found in the network layer. When the hello packets that are utilized for neighbor discovery are sent or replayed, an attack is caused due to the higher consumption of power which is known as hello flood attack. An illusion is created by the attacker node as being one of the neighbors of other nodes due to which the other attacks can also enter the network as the routing protocol can completely be disrupted in this scenario [3], [15], [16]. The attack that is caused due to the generation of low-latency link such that the packets take a multi-hop route in order to travel amongst each other is known as wormhole attack. The routing protocol is affected through this attack and it needs to be identified and eliminated from the network. An attack in which several entities are generated by the malicious node such that the network traffic can be affected directly is known as Sybil attack. An attack that is caused when complete and accurate sensing data is prevented from reaching the base station is known as sinkhole attack. The higher-layer applications also are prone to serious threat due to this attack. Almost all the traffic from particular area is attracted

towards the attacker due to this attack. Flooding attack is a type of transport layer attack. Large amount of traffic is flooded in order to bring network or service down in this Denial of Service type of attack known as flooding attack. In case when a network or service is weighed down with the packets, the network is more likely to have flood attacks [4], [17], [18]. The actual connection requests can thus no longer be processed in this case. Denial-of-service (DoS) and cloning are two application layer attacks. An intended attack caused by opponents in order to destroy the complete sensor network is known as Denial-of-Service attack. The expected functionality of the sensor network is destructed due to the presence of this attack. Within any of the layers of OSI architecture of WSN, this type of attack can enter. When the sensor nodes are easily captured and compromised and unlimited numbers of clones are deployed within the sensor network of the compromised nodes, the attack generated is known as cloning attack. Sybil Attack: An attack that is generated due to the creation of multiple identities from similar malicious node is known as Sybil attack. Since, several other types of attacks can also be generated due to this type of attack; the WSNs are highly vulnerable to this attack [5], [21]. Within the distributed storage, voting as well as resource allocation, there are higher numbers of issues that arise in WSNs due to this type of attack. It is not possible for the sensor networks to introduce security mechanisms within their scenarios on their own due to their structure. Thus, in order to enhance the security of sensor networks, a better security mechanism is proposed such that WSN can be protected from this type of attack [6], [19], [20]. On the basis of communication, simultaneity as well as fabricated identities, the Sybil attack can be generated in WSNs. It is seen that a malicious node can gain access to the normal node when one hop communication is being performed during the communication of nodes. The detailed information of the normal node can all be known to this malicious node which can be utilized in order to generate similar identities. Due to this, there will lots of confusion caused in the network and the complete network will be corrupted resulting in causing Sybil attack [22].

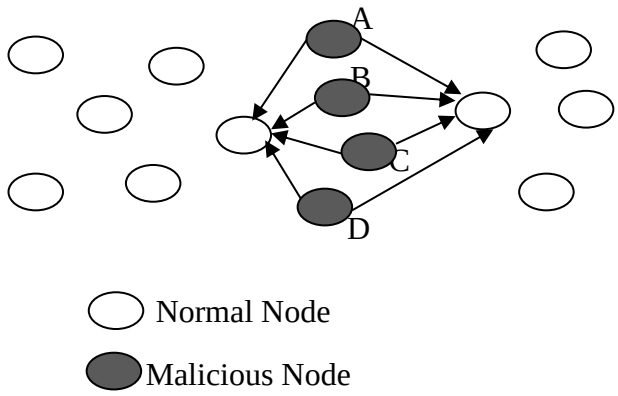

Fig. 1: Sybil Attack in WSN.

2. Related work

Qihao Li, et.al proposed a novel approach to identify Sybil attack within WSNs [7]. Figure 1 shows sybil attack in WSN. The spatial variability from the channel responses is exploited through which the power gain and delay spread analysis is performed in order to propose this approach. In order to represent the characteristics of sensors on the basis of power gain and delay spread that is attained from channel response, the channel-vectors are utilized here. In order to differentiate Sybil attackers from genuine sensors, a kernel-oriented method is generated. Simulations performed and results achieved show that there is higher level of accuracy achieved through the proposed approach is terms protecting packets from the Sybil attackers. Noor Alsaedi, et.al presented the issues being faced when a lightweight trust system is generated. In order to address this issue for hierarchical WSN, a metric parameter that utilized energy is proposed [8]. It is seen through the performance evaluations that for the detection of Sybil attacks with respect to true and false positive identifications, the results achieved as highly efficient and scalable. In addition, through the elimination of feedback and recommendations amongst the senor nodes, the communication overhead is minimized in this system. Salavat Marian, et.al proposed a novel robust and lightweight approach based on RSSI (received signal strength indicator) that is utilized for detecting the Sybil attacks in WSN [9]. Received Signal Strength Indicator and Link Quality Indicator (LQI) are the two known indicators that are utilized for link quality estimation in WSNs lately. Within the static environments and with the presence of good transceivers also it is seen that RSSI performs in very stable manner. Here, the Sybil nodes are localized with the help of received power. Sepide Moradi, et.al proposed a novel technique for WSNs in order to identify the Sybil attacks [10]. This approach uses mobile nodes within the routing mechanism instead of including adversary nodes. Thus, the security of the network is enhanced. Better performance results have been achieved as per the results achieved through simulations. Also, the packet loss rate and additional overhead are also minimized through this approach. Panagiotis Sarigiannidis, et.al presented an accurate performance analysis of the indirect Sybil attacks generated within the WSNs [11]. The probability of elimination of availability of potential indirect Sybil attacks in the network is described through rigorous close equations. In order to establish zero probability of including the potential indirect Sybil nodes within the network, necessary numbers of sensor nodes within particular area are identified. Further, computation of expected number of potential indirect Sybil nodes is also done in similar manner. Thus, the results are analyzed and enhancement in results is seen through comparisons in proposed and already existing approaches.

3. Proposed methodology

In the wireless sensor network, sensor nodes can connect or dissert the network anytime when they want due to property of decentralization. Presence of malicious node within the network is responsible of triggering active and passive attacks this is due to dynamic nature of the networks. The network performance in terms of certain parameters has been affected by the active attacks. The Denial of service is the active type of attack in which malicious node flood the legitimate nodes with the rough packets to reduce network performance. The distributed denial of service is the advance type of DOS attack in which malicious node choose its slave and slaves will flood the legitimate node which the rough packets and it reduce network performance. This research work, is based on the detection and isolation of malicious nodes from the network which are responsible to trigger sybil attack in the network. In the proposed technique, the key servers are formed in the network and each node in the network will register itself to the key server node with their data rate and bandwidth consumption. When all the nodes start transmitting data in the network, and when the sybil attack is triggered in the network and throughput of the network get reduced to threshold value then malicious node detection process starts. In the process of malicious node detection, the nodes which are sending data above the threshold value are considered as malicious node and technique of watch dog is applied that whether these nodes are sending data packets or control packets. When the nodes are sending the data packets, then that nodes are considered as the slave nodes. The technique of monitor mode is applied on the slave nodes which can then analyze the network traffic. When the slave nodes receive the control packets from the other node, then the node which send control packet is detected as the malicious node in the network. The proposed technique is applied under the simulated environment so that presence of malicious nodes can be determined easily which is responsible of causing sybil attack in the network.

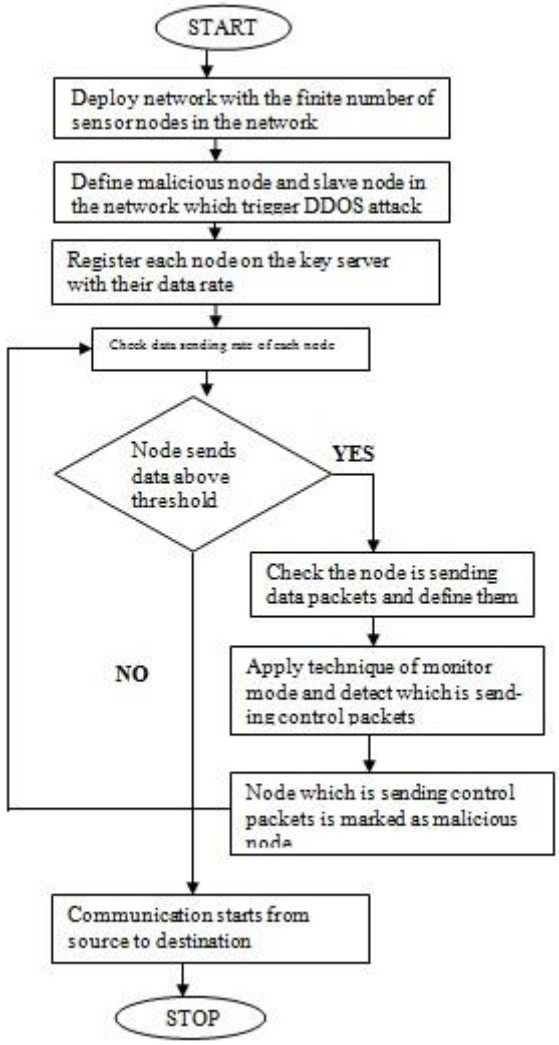

Fig. 2: Proposed Methodology.

4. Simulation parameters

TCL programming environment is used in order to perform simulations. AODV routing protocol is utilized within the simulation. Further, CSMA/CA protocol is utilized in order to avoid collision within the media access. Two different scenarios are considered here for performing simulations. Without including proposed securing mechanism, simulation for initial scenario is performed. Further, the secondary simulation is performed by including the proposed algorithm in it. The parameters included in simulation are presented in Table 1.

Table 1: Parameters of Simulation

Parameter	Value
Simulation time	20 min
Network Scale	200mX200m
MAC protocol	CSMA/CA
Routing protocol	AODV
Transmission Range	50
Mobile agent code size	512 byte
Packet size	512 byte
Speed	10 m/s

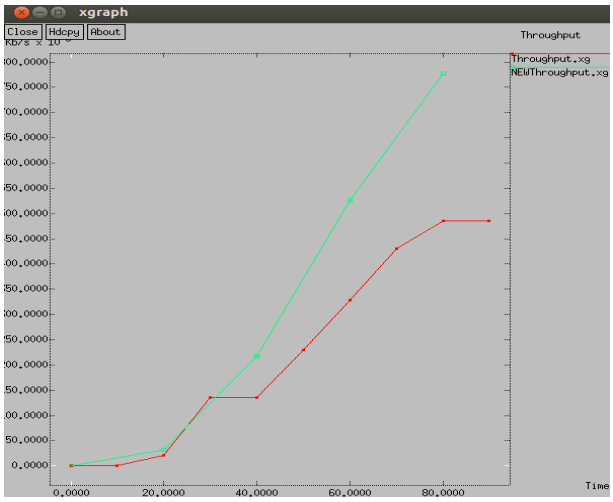

Fig. 3: Throughput Comparison.

As shown in figure 3, the throughput of the proposed scenario is compared with the existing scenario. It is analyzed that when attack is isolated from the network, then throughput is increased at steady rate

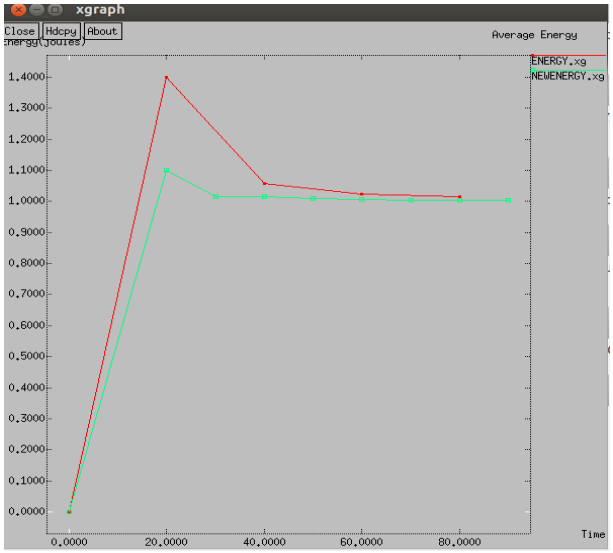

Fig. 4: Energy Consumption.

As shown in figure 4, the sensor nodes has very small size and it is self configuring in nature. Due to which energy consumption need to reduce to increase network lifetime. In this graph the energy consumption graph is represented.

5. Conclusion

In this work, it is concluded that wireless sensor network is the decentralized type of network due to which security is the major issue of wireless sensor network. This research work is based on detection and isolation of Sybil attack in the network. The technique is proposed in this research work which is based on the mutual authentication technique for the detection of mutual authentication. The simulation of proposed model is performed in NS2 which shows up to 20 percent improvement in the results

References

[1] M. Cheffena, "Industrial wireless communications over the millimeter wave spectrum: opportunities and challenges," IEEE Commun., vol. 54, no. 9, pp. 66–72, 2016.
[2] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the internet of things," IEEE J. on Internet of Things, vol. 1, no. 5, pp. 372–383, 2014.

[3] I. Butun, S. Morgera, and R. Sankar, “A survey of intrusion detection systems in wireless sensor networks,” IEEE Commun. Surveys & Tutorials, vol. 16, no. 1, pp. 266–282, 2014.
[4] Q. Xiong, Y. Liang, K. Li, and Y. Gong, “An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems,” IEEE Trans. on Inf. Forens. In addition, Security, vol. 10, no. 5, pp. 932–940, 2015.
[5] S. Ruj, A. Nayak, and I. Stojmenovic, “Pairwise and triple key distribution in wireless sensor networks with applications,” IEEE Trans. Comput., vol. 62, no. 11, pp. 2224–2237, 2013.
[6] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, “Channel-based detection of sybil attacks in wireless networks,” IEEE Trans. Inf. Forens. Security, vol. 4, no. 3, pp. 492–503, 2009.
[7] Qihao Li, Kuan Zhang, Michael Cheffena and Xuemin (Sherman) Shen, “Channel-based Sybil Detection in Industrial Wireless Sensor Networks: a Multi-kernel Approach”, 2017, IEEE.
[8] 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).
[9] 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
[10] 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).
[11] 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.
[12] Roshan Singh Sachan, Mohammad Wazid, AvitaKatal, D P Singh, R H Goudar, “A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack in-side WSN”, International conference on Communication and Signal Processing, April 3-5, 2013, India.
[13] G. Padmavathi, Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechan-isms andChallenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.
[14] Kalpana Sharma and M K Ghose, “Wireless Sensor Networks: An Overview on its Se-curity Threats” IJCA Special Issue on “Mobile Ad-hoc Networks”MANETs, 2010.
[15] LVShaohe, Wang Xiaodong, Zhao Xing," Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", Computational Intelligence and Security 2008,CIS '08 In-ternational Conference on Volume 1Suzhou,pp.442-446,IEEE 2000.
[16] Baviskar B.R, Patil V.N," Black hole attacks mitigation and prevention in wireless sensor network", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp.167-169, May 2014.
[17] Wang Chun-Hsin and Li Yang-Tang, “Active Black Holes Detection in Ad-Hoc Wire-less Networks”, Ubiquitous and Future Networks (ICUFN) 2013 Fifth International Conference on Da Nang, pp.94-99, IEEE, 2013.
[18] Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, Ali Farrokhtala, “ Detection of sink hole Attack in wireless sensor networks”, IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia.
[19] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha,” Intru-Sion Detection in Wireless Ad Hoc Networks”, 2004 Ieee 1536-1284-04.
[20] Ju young Kim, Ronnie D. Caytiles, Kyung Jung Kim, “A Review of the Vulnerabilities and Attacks for Wireless Sensor Networks” Journal of Security Engineering, 2014.
[21] Kalpana Sharma and M K Ghose, “Wireless Sensor Networks: An Overview on its Se-curity Threats” IJCA Special Issue on “Mobile Ad-hoc Networks”MANETs, 2010.
[22] M.Santhanalakshmi, T.Anushapriya,LathaMathavan Engineering,” An Effective Hybrid intrusion detection system for large scale wireless sensor networks”, 2016.