SYBIL ATTACK COUNTERMEASURES IN WIRELESS SENSOR NETWORKS

Rupinder Singh[†], Dr. Jatinder Singh[‡], and Dr. Ravinder Singh[‡]

[†]*Research Scholar, IKG PTU, Kapurthala, Punjab.*
[‡]*IKG PTU, Kapurthala, Punjab.*
E-mail: [†] rupi_singh76@yahoo.com, [‡]bal_jatinder@rediffmail.com

Abstract - A wireless sensor network (WSN) is a network formed by a large number of sensor nodes, where each node is equipped with a sensor in order to detect physical phenomena such as pressure, light, heat, etc. WSNs are regarded as a revolutionary information gathering system to build the information and communication system which will greatly improve the reliability and efficiency of infrastructure systems. WSN play an important role in the controlling and managing of environments in different situations and has become important part of research area. WSN research is basically classified into three categories i.e. hardware & software of the sensors nodes, application area, and communication & security. Due to limited resources of battery, computation power, communication range etc., WSN are vulnerable to different types of attacks. Sybil attack is one of such attack in which a node illegitimately takes multiple identities or claims fake IDs. In this paper we first describe the sybil attack and then we discuss different techniques/mechanisms proposed in the literature for tackling with it. A detail study of these techniques and their limitations will help in the design of novel, robust and more efficient techniques for tackling with sybil attack, so that the applications of sensor nodes can be extended to other fields.

Keywords: Wireless sensor network, Sensor, Vulnerable, Sybil attack, illegitimately.

I. INTRODUCTION

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

The need for more effective security mechanisms is increasing due to continue growth of wireless sensor networks. The security issues of the sensor network should be addressed from the beginning of designing of the system, since sensor networks interact with sensitive data and usually operate in a hostile unattended environment. A detailed study of the capabilities and limitations of each of the underlying technology is required for secure working of WSN. Every node in the WSN should be designed in order to provide the set of primitives that are necessary to synthesize connected topology as it is deployed. This is required to meet the strict condition of power consumption, size, and cost for WSN. Apart from this, security for group communications applications that require packet delivery from one or more senders to multiple receivers is a more critical and challenging goal.

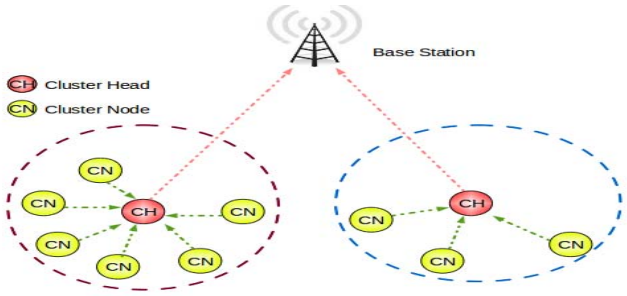

Figure 1: A typical WSN

The security challenges of WSN are totally different from traditional network security due to the limitation of resources and computing capabilities. Sensor nodes are usually deployed in large accessible areas that present the added risk of physical attack. Sensor networks also poses new security problems as they interact closely with their physical environments and with people. Most of the techniques proposed in the past assumed that all the nodes are cooperative and trustworthy. However, today, this is not the case for most of the sensor network applications, that require a certain amount of trust in the application. This is needed in order to maintain proper network functionality. Consequently, the security mechanisms existing are inadequate resulting in new ideas and new research directions for properly addressing sensor network security.

A number of attacks are possible in WSN including hello flood, wormhole, sybil, jamming, tampering, collision, exhausting, sinkhole, flooding, denial-of-service, cloning etc. The WSN suffers from an attack called sybil attack in which the node replicates itself to make many copies to confuse and collapse the network. In this paper we first describe the Sybil attack and then we discuss different techniques / mechanisms proposed in the literature for tackling with it. A detail study of these techniques and their limitations will help in the design of novel, robust and more efficient techniques for tackling with sybil attack, so that the application of sensor nodes can be extended to other fields.

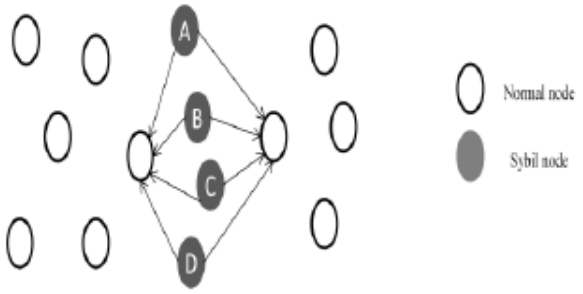

Figure 1: Sybil attack in WSN

II. SYBIL ATTACK

The WSN suffers from an attack called sybil attack in which a node illegitimately claims multiple identities or claims fake IDs. In order to collapse the network, in sybil attack, malicious node replicates itself to make many copies to confuse. The system can be attacked externally or internally. Prevention of external attacks can be done by authentication but the same cannot be done with internal attacks. The mapping between identity and entity in WSN should be one to one, but sybil attack by creating multiple identities violates this one-to-one mapping.

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.

III. SYBIL ATTACK COUNTERMEASURES

In this section of the paper, we provides various countermeasures proposed in the literature to tackle with the sybil attack in wireless sensor networks.

A. Message Authentication and Passing Method

According to authors in [1], 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 CAM-PVM 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 [2]. 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 [3]. This method facilitates deployment and control of the positions of the nodes and thereby it prevent 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 [4]. 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 ranges to 16%.

E. SYBILSECURE technique

An energy efficient algorithm named Sybilsecure is proposed in [5]. According to the authors, experimental results show that Sybilsecure consumes less energy as compare to the existing defense mechanisms. Sybilsecure 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 sybilsecure , 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-E-GA in [6]. 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 [7] 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 indicator 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 presentes a dynamic, distributed algorithm for the detection of sybil nodes in wireless sensor networks.

H. P^2DAP approach

A lightweight and scalable protocol to detect sybil attacks is provided in [8]. 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 security, 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 [9]. 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 [10]. 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 [11]. 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 [12]. 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 [13]. 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 shows 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 [14] 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 [15]. 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 [16]. 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 sytem 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 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.

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. In this paper we first discuss in detail the sybil attack, and then we provide in detail different techniques / mechanisms proposed for tackling with sybil attack in the literature. 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.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] R. Amuthavalli & R. S. Bhuvaneswaran , " Genetic Algorithm Enabled Prevention of Sybil Attacks for LEACH-E," Modern Applied Science; Vol. 9, No. 9; 2015, ISSN 1913-1844 E-ISSN 1913-1852.

[7] 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.

[8] 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.

[9] A. V. Vibi, G. V. Padmasree, P. Nithya, and C. Geetha, "Detection of sybil attack using neighbouring 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.

[10] 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.

[11] 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.

[12] Krishna Kumar, V.Shalini, V.Shiva and P.Vijayakanth, "Detection And Prevention of Sybil Attack Using A Thershold Elgamal Key Management Scheme," International Journal of Advances in Engineering, 2015, ISSN: 2394-9260.

[13] Prameet Kaur and Dr. Sandeep Singh Kang, " Optimized secure routing protocol to prevent sybil attack in wireless sensor networks," International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013, ISSN 2229-5518.

[14] Murat Demirbas and Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks,"www.cse.buffalo.edu/tech-reports/2006-01.pdf

[15] Liang Xiao, Larry J. Greenstein, Narayan B. Mandayam, and Wade Trappe, "Channel-Based Detection of Sybil Attacks in Wireless Networks," IEEE Transactions on information forensics and security, Vol. 4, No. 3, September 2009.

[16] 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.

[17] Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN," International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.

[18] Jatinder Singh , Dr. Savita Gupta , and Dr. Lakhwinder Kaur , " A Cross - Layer Based Intrusion Detection Technique for Wireless Networks , " The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012.