A Study on Efficient Defense Mechanism Against Sybil Attack in WSN

Anil
Research Scholar
Department of Computer Science and Engineering
Ganga Institute of Technology & Management, Kablana

Yashpal Singh
Assistant Professor
Department of Computer Science and Engineering
Ganga Institute of Technology & Management, Kablana

Abstract

Sensor network consists of tiny sensors and actuators with general purpose computing elements to cooperatively monitor physical or environmental conditions, such as temperature, pressure, etc. Wireless Sensor Networks are uniquely characterized by properties like limited power they can harvest or store, dynamic network topology, large scale of deployment. Sensor networks have a huge application in field which includes habitat monitoring, object tracking, redetection, land slide detection and monitoring. As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. While there are many types of security attacks in WSNs, we have decided to focus our analysis on a particularly harmful one: the Sybil attack. A Sybil attack succeeds when a malicious node, called the Sybil node, illegitimately claims multiple false identities by either fabricating new identities or impersonating existing ones. The goal of a Sybil attack is to gain a disproportionate amount of influence over the network via its false identities. Now Sybil attack has caused too much threaten to wireless sensor network in routing, voting system, fair resource allocation, data aggregation and misbehavior detection. Hence many methods are being proposed to detect and prevent Sybil attack in wireless sensor network. A detailed study of these methods has been carried out and comparison table gives an overview of the method's performance. Conclusions have been drawn using the comparison table. Parameters show how the method performs. Simulation work is performed on NS2 simulator. We have implemented the simple form of Sybil attack and an algorithm is proposed to detect Sybil attack. Performance evaluation is done using the packet delivery ratio, number of packets generated. The results shows that packet delivery ratio and number of packets generated for Sybil nodes are same in each scenario.
Keywords: WSN, NS2 simulator, Sybil attack

I. INTRODUCTION

Wireless sensor network is a collection of nodes (sensors) organized into a cooperative network [1]. Each node consists of processing capability (one or more microcontrollers, CPUs or DSP chips), may contain multiple types of memory (program, data and flash memories), have a RF transceiver (usually with a single omnidirectional antenna), have a power source (e.g., batteries and solar cells), and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. These tiny sensors have the ability of sensing, data processing, and communicating with each other. Wireless Sensor Networks (WSN) which rely on collaborative work of large number of sensors are realized. Sensor nodes can be used within many deployment scenarios such as continuous sensing, event detection, event identification, location sensing, and local control of actuators for a wide range of applications such as military, environment, health, space exploration, and disaster relief. Although a large volume of research has been performed and some algorithms are proposed, there is ongoing research on this subject in recent years [2].

One of the challenging subjects and design constraints in WSNs is security. Because sensor nodes have limited storage and computational resources, it can easily be assaulted. Various types of attacks such as wormhole attack, sinkhole attack, selective forward attack, Sybil attack can be present in a network. A particularly harmful attack against sensor networks is the Sybil attack as this attack can make the network easily vulnerable to other attacks. Sybil attack is where a node illegitimately claims multiple identities. Now Sybil attack has caused too much threaten to wireless sensor network in routing, voting system, fair resource allocation, data aggregation and misbehavior detection. Hence many methods are being proposed to detect and prevent Sybil attack in wireless sensor network.

Wireless Sensor Networks are characterized by:

- Limited power they can harvest or store.
- Ability to cope with node failures.
- Heterogeneity of nodes.
- Large scale of deployment.
- Mobility of nodes.

- Communication failures.
- Dynamic network topology.
- Ability to withstand harsh environmental conditions.

A. Architecture of wsn

In a common WSN architecture (fig1.1), the measurement nodes are deployed to acquire measurements such as temperature, voltage, or even dissolved oxygen. The nodes are part of a wireless network administered by the gateway, which governs network aspects such as client authentication and data security. The gateway collects the measurement data from each node and sends it over a wired connection, typically Ethernet, to a host controller. There, software such as the NI Lab VIEW graphical development environment can perform advanced processing and analysis and present your data in a fashion that meets your needs.

The main components of a sensor node (fig 1.2) are a microcontroller, transceiver, external memory, power source and one or more sensors.

1) Controller:

The controller performs tasks, processes data and controls the functionality of other components in the sensor node. While the most common controller is a microcontroller, other alternatives that can be used as a controller are: a general purpose desktop microprocessor, digital signal processors.

2) Transceiver:

The functionality of both transmitter and receiver are combined into a single device known as a transceiver. Transceivers often lack unique identifiers. The operational states are transmit, receive, idle, and sleep. Current generation transceivers have built-in state machines that perform some operations automatically.

3) External Memory:

From an energy perspective, the most relevant kinds of memory are the on-chip memory of a microcontroller and Flash memory—off-chip RAM is rarely, if ever, used. Flash memories are used due to their cost and storage capacity. Memory requirements are very much application dependent. Two categories of memory based on the purpose of storage are: user memory used for storing application related or personal data, and program memory used for programming the device. Program memory also contains identification data of the device if present.

4) Power Source:

The sensor node consumes power for sensing, communicating and data processing. More energy is required for data communication than any other process. Power is stored either in batteries or capacitors. Batteries, both rechargeable and non-rechargeable, are the main source of power supply for sensor nodes.

5) Sensors:

Sensors are hardware devices that produce a measurable response to a change in a physical condition like temperature or pressure. Sensors measure physical data of the parameter to be monitored. The continual analog signal produced by the sensors is digitized by an analog-to-digital converter and sent to controllers for further processing.

A sensor network normally constitutes a wireless ad-hoc network, meaning that each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station).

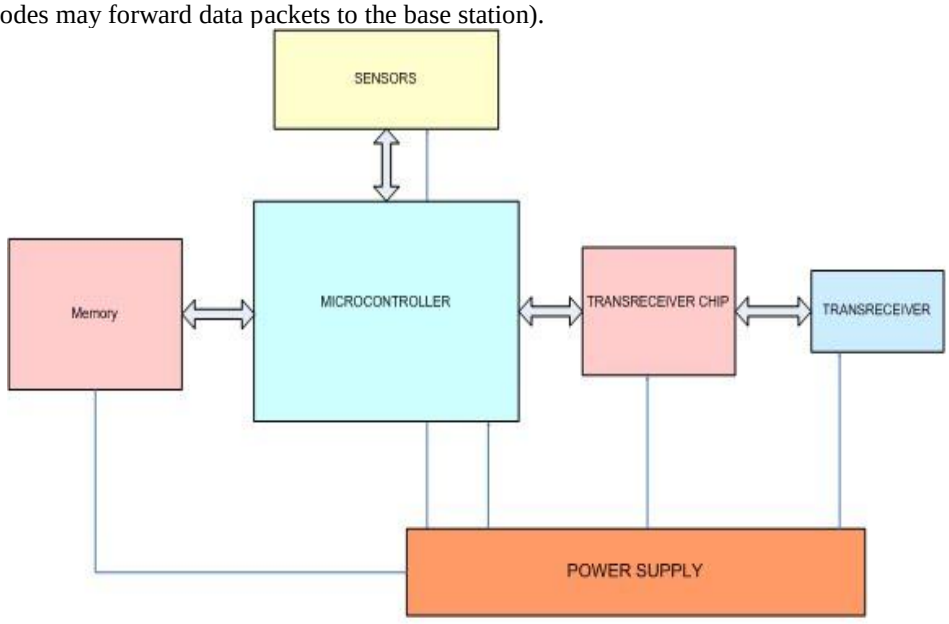

Fig. 2.2: Major components of a sensor node

II. REVIEW OF LITERATURE

A. Security of wireless sensor networks (Daniel E. Burgner, Luay A. Wahsheh)

The research reviewed in this paper represents the tip of the iceberg when it comes to the security of wireless sensor networks. Architectures play a key purpose in wireless sensor networks as do unique security issues such as how security affects context and design matters as well as working with confidentiality, integrity, and authenticity. Algorithms also have a role in the process of constructing a wireless sensor network. Lastly, performance issues are addressed to determine if such a proposed design is feasible for use. Based on security analysis of all the wireless sensor networks, it is concluded that SOWSN has the best performance since it is based on real scenarios. More research in this area will continue as it is an emerginz technology for years to come.

B. Defending against Sybil attack in sensor networks (Qinghua Zhang, Pan Wang, Douglas S. Reeves, Peng Ning)

In a Sybil attack, a single node illegally presents multiple identities to other nodes. This paper proposes a method of defending against such attacks in sensor networks. The method uses a two-level Merkle hash tree to create certificates. An interactive node-to-node authentication protocol employs one-way key chains for message authentication. This method does not require clock synchronization between nodes, and is robust against man-in-the middle attacks. An extension of this method exploits node deployment knowledge to reduce the computational overhead at each node. This extended method is substantially more scalable, with a small reduction in the security it provides.

C. The Sybil Attack in Sensor Networks: Analysis & Defenses (James Newsome, Elaine Shi, Dawn Song, Adrian Perrig)

In this paper, they define the Sybil attack and establish a taxonomy of this attack by distinguishing different attack types. The definition and taxonomy are very important in understanding and analyzing the threat and defenses of a Sybil attack. They present several novel methods by which a node can verify whether other identities are Sybil identities, including radio resource testing, key validation for random ke predistribution, position verification and registration. The most promising method among these is the random key predistribution which associates a node's keys with its identity. Random key predistribution will be used in many scenarios for secure communication, and because it relies on well understood cryptographic principles it is easier to analyze than other methods. These methods are robust to compromised nodes. In particular, they have shown that in the multi-space pairwise scheme with each node storing 200 keys, the attacker would need to compromise 400 nodes before having even a 5% chance of being able to fabricate new identities for the Sybil attack.

D. Wireless sensor network: A survey(John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary)

In this chapter they have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories they have also sub-categorized the major topics including routing, trust, denial of service, and so on. Their aim is to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher.
As wireless sensor networks continue to grow and become more common, they expect that further expectations of security will be required of these wireless sensor network applications. In particular, the addition of public key cryptography and the addition of public-key based key management will likely make strong security a more realistic expectation in the future. They also expect that the current and future work in privacy and trust will make wireless sensor networks a more attractive option in a variety of new arenas.

E. Detection of sybil attack in mobile wireless sensor networks (S.Sharmila, G Umamaheswari)

A number of existing methodologies for the detection of Sybil attack have been studied and an algorithm is proposed for detection of Sybil attack in wireless sensor network. The throughput and packet delivery ratio of the network, before and after detection is analysed for different traffic rates. It is found that throughput and packet delivery ratio after detection has improved.

F. Wireless sensor networks For security: Issues and challenges (Tolga Onel, Ertan Onur, Cem Ersoy and Hakan Delic)

They employ the Neyman-Pearson detector to find the sensing coverage area of the surveillance wireless sensor networks. In order to find the breach path, they apply Dijkstra's shortest path algorithm by using Mthe negative log of the miss probabilities as the grid point weights. The breach probability is defined as the miss probability of the weakest breach path. The false alarm rate constraint has a significant impact on the intrusion detection performance of the network, which is measured by the breach probability. The model and results developed herein give clues that link false alarms to energy efficiency. Enforcing a low false alarm rate to avoid unnecessary response costs implies either a larger data-set (L) and hence greater battery consumption, or a denser sensor network, which increases the deployment cost. Similar qualitative and/or quantitative inferences about the relationships between various other parameters can also be made. Wireless sensor networks are prone to failures. Furthermore, the sensor nodes die due to their limited energy resources. Therefore, the failures of sensor nodes must be modelled and incorporated into the breach path calculations in the future. Simulating the reliability of the network throughout the entire life of the wireless sensor network is also required.

Lastly, especially for perimeter surveillance applications, obstacles in the environment play a critical role in terms of sensing and must be incorporated in the field model.

A mutual information based information metric is adopted to select the most informative subset of sensors to actively participate in the distribute data fusion framework. The duty of the sensors is to accurately localize and track the targets. Simulation results show 36% energy saving for a given tracking quality can be achievable by selecting the sensors to cooperate according to the mutual information metric. In all tests, they assumed all the sensor nodes send reliable data to the network. In future work, detection of faulty and outlier sensors in the network must be investigated, and precautions need to be taken against them. They considered the effect of sensor selection algorithms in the context of distributed data fusion for tracking a single target. Existence of multiple targets introduces challenges with track-to-track association and track-to-sensor association, as well as issues related to access control and routing.

G. Security Analysis on Defenses against Sybil Attacks in Wireless Sensor Networks (Karen Hsu, Man-Kit Leung, Brian Su)

They have evaluated a wide range of defenses against the Sybil attack in wireless sensor networks using five metrics: resiliency, connectivity, processing complexity, storage complexity, and communication complexity. Often times, these metrics alone are not enough to determine the usability of a particular defense, although they do aid in gauging the security and practicality tradeoffs. For example, radio resource testing has reasonable metric values. However, it is deemed unusable due to its requirement of each node having only one radio. Similarly with code attestation, it requires the attacker to go through great lengths to forge multiple identities in order to perform a Sybil attack. However, its current proposed use to detect a Sybil attack (i.e. computation time) is not a very reliable method as many factors can contribute to this (i.e. regular network delays). On the other hand, location verification has perfect resiliency and is, of all the defenses, most likely to handle dynamic network topologies. However, extra communication overhead is required in order to perform location validations. Moreover each node is required to rely on its observers; if a Sybil attack had already succeeded, the Sybil node can lie about the location of other Sybil nodes to thwart detection. Key-based methods seemed most suitable to our metrics - ECC is a promising asymmetric key cryptography solution due to its shorter key-length requirement. Additionally, public key authentication offers high connectivity and high resiliency, both very desirable traits. More research in this area should show promising results. As for pairwise key predistribution schemes, in order to protect sizeable networks, one always has to deal with the key management problem. Multi-space schemes, including location-based schemes, work best for such large networks but require dense node population. Similarly, probabilistic models also require dense, uniform networks. Moreover, it performs poorly in both resiliency and connectivity. They consider polynomial-based schemes to be an improvement over matrix-based schemes as they offer the same resiliency and connectivity, but necessitate less storage and less communication overhead.

H. An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks (Murat Demirbas, Youngwhan Song)

They presented an RSSI-based solution for the Sybil attack problem in WSN. They showed that even though RSSI is time varying and unreliable in general and radio transmission is non-isotropic, using ratio of RSSIs from multiple receivers it is feasible to overcome these problems. Our protocol is lightweight—alongside the receiver they need the collaboration of one other node— and robust—they achieve detection with 100% completeness and less than a few percent false positives.

I. A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks (Shio Kumar Singh , M P Singh , and D K Singh)

Security is becoming a major concern for energy constrained wireless sensor network because of the broad security-critical applications of WSNs. Thus, security in WSNs has attracted a lot of attention in the recent years. The salient features of WSNs make it very challenging to design strong security protocols while still maintaining low overheads. In this paper, they have introduced some security issues, threats, and attacks in WSNs and some of the solutions. Network security for WSNs is still a very fruitful research direction to be further explored.

J. A Review of Techniques to Mitigate Sybil Attacks (Nitish Balachandran, Sugata Sanyal)

In this paper, they have discussed the important kinds of Sybil attacks that can be launched on various application domains. They have also listed notable methods that have been proposed over time to tackle these attacks. Further, they have elaborated on their modus operandi, advantages, and limitations.

K. Security Framework for Wireless Sensor Networks (Neeli r. Prasad and Mahbubul Alam)

This paper analyses the security issues, threats and attacks and requirements of wireless sensor networks. This paper further proposes security framework and security architecture to integrate existing technologies with WSN technology, to provide secure and private communications to its users.

L. A Survey on Wireless Sensor Networks Security (Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti)

The paper presented a concise survey on sensor network constraints, security requirements, attacks and defensive measures. As noted, security requirements are critical to preventing an adversary from compromising the security of a distributed wireless

sensor network. The key establishment protocols and approaches for distributed wireless sensor networks must satisfy several security and functional requirements.

M. Wireless sensor network security analysis (Hemanta Kumar Kalita and Avijit Kar)

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a full proof security to the network. In this paper, they have made a threat analysis to the Wireless Sensor Network and suggested some counter measures. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

III. ALGORITHM USED

The following algorithm has been proposed:

A. Phase I:

1) Take some (15) trust nodes.
2) Add few (5) nodes to the network of trust nodes. These new added nodes can be Sybil or trust nodes.
3) Transfer the data from new added nodes to the trust nodes.
4) Calculate the packet delivery ratio and number of packets generated in the given amount of time.
5) Retrieve the Sybil nodes on the basis of step 4 (Sybil nodes will have nearly same packet delivery ratio and number of packets generated).

B. Phase II:

1) Choose distant trust nodes.
2) Sybil nodes of phase I will transfer data to the trust nodes.
3) On the basis of path followed, determine the Sybil nodes (Sybil nodes detected in previous phase will follow the same path to send data to any particular node).

C. Phase III:

1) Send the packets between the new added nodes of phase I.
2) On the basis of number of hops between the nodes, find out the Sybil nodes.
3) If there is no any hop between two nodes, then these will be Sybil nodes.

IV. SIMULATION

Initially only simple form of Sybil attack is presented. Here a network is established with 31 nodes. We want to send data from node 0 to node 10, 11 and 20 which are our destination nodes. In one scenario, there is no attack, hence all data is going to destination nodes. But in second scenario, node 10,11 and 20 are fake IDs of node 15, hence all data is going to node 15 instead of 10,11 and 20.

A. Initial creation of 32 nodes

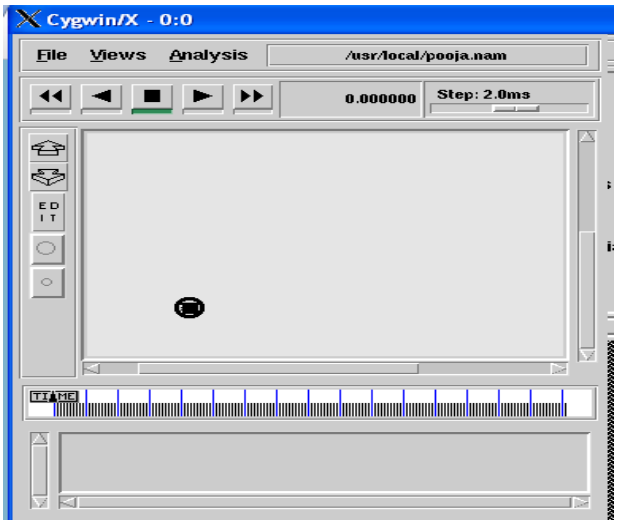

Fig. 5.1: Simulation Result 1

Movement of nodes to their respective positions.

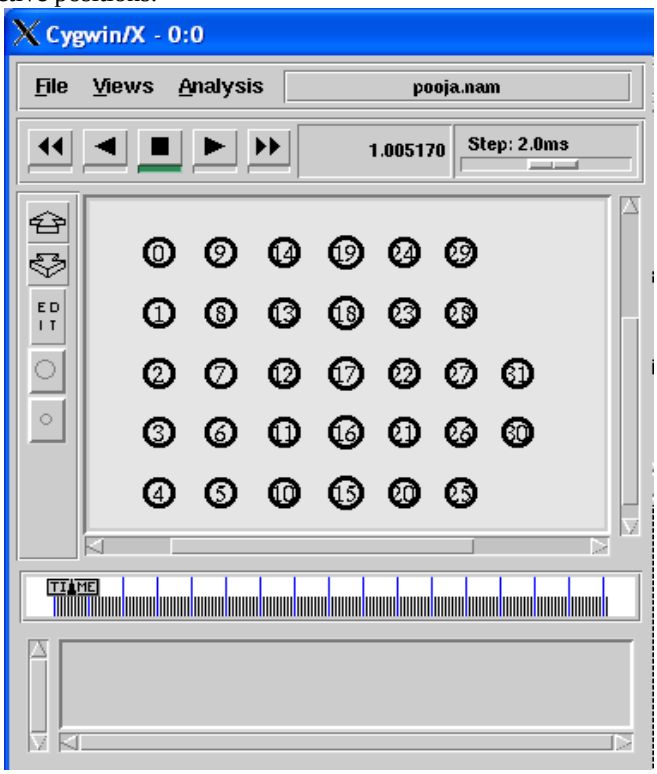

Fig. 5.2: Simulation Result 2

Transfer of data to nodes 10,11 and 20 without Sybil attack. All data is going to their destinations.

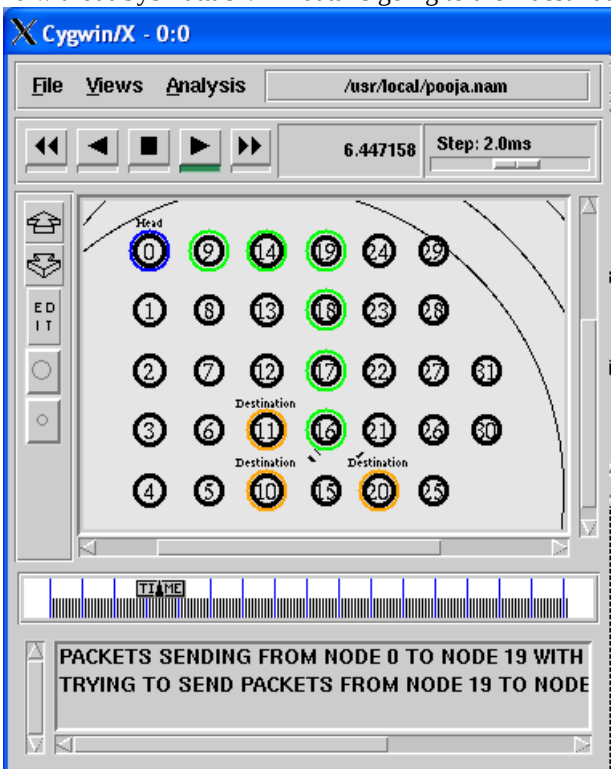

Fig. 5.3: Simulation Result 3

Trying to send packets from node 0 to node 19 and then from node 19 to node 11,12 and 20.
But 11,12 and 20 are fake IDs of node 15. Hence all data is going to node 15 due to Sybil attack.

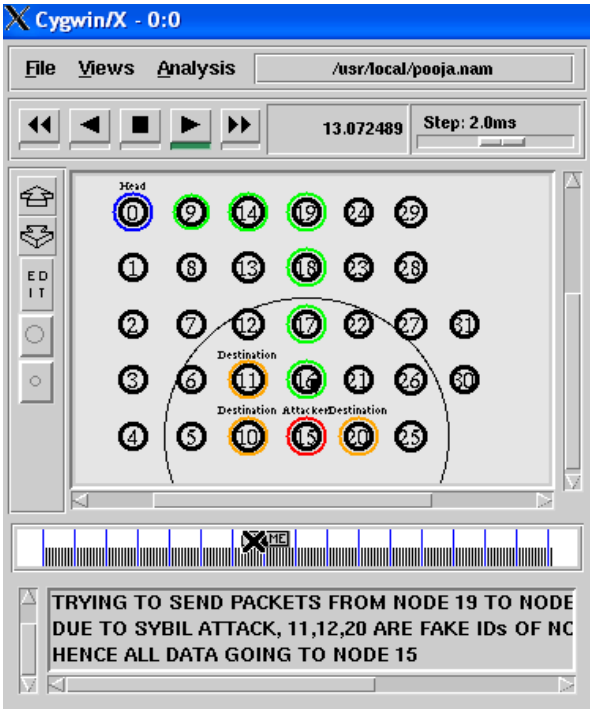

Fig. 5.4: Simulation Result 4

V. CONCLUSION

In this work we explain various security attacks of wireless sensor networks. Then we focus on particular harmful attack- Sybil attack. We define the Sybil attack and establish taxonomy of this attack by distinguishing different attack types. We define the Sybil attack as a malicious device illegitimately taking on multiple identities. The definition and taxonomy are very important in understanding and analyzing the threat and defenses of a Sybil attack. We have discussed the important kinds of Sybil attacks that can be launched on various application domains. We have also listed notable methods that have been proposed over time to tackle these attacks. The main methods discussed are: Trusted Certification, Resource Testing, Radio Resource Testing, RSSI-based scheme, Random key predistribution, Location/Position verification.

REFERENCES

[1] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System Architecture Directions for Networked Sensors. ASPLOS, November 2000.
[2] A. Savvides, C.-C. Han, and M. Srivastava. Dynamic Fine-Grained Localization in Ad-Hoc Networks of Sensors. Proc. 7th ACM MobiCom, July 2001, pp. 166–79.
[3] Weichao Wang, Di Pu and Alex Wyglinski. Detecting Sybil Nodes in Wireless Networks with Physical Layer Network Coding. IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), 2010.
[4] S. Sharma, Energy-efficient Secure Routing in Wireless Sensor Networks. Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.
[5] D. Boyle, T. Newe, Securing Wireless Sensor Networks: Security Architectures. Journal of Networks, 2008, 3 (1).
[6] X. Du, H. Chen. Security in Wireless Sensor Networks. IEEE Wireless Communications, 2008.
[7] J. Granjal, R. Silva, J. Silva, Security in Wireless Sensor Networks. CISUC UC, 2008.
[8] Jun Zheng and Abbas Jamalipour. Wireless Sensor Networks: A Networking Perspective. A book published by A John & Sons, Inc, and IEEEE, 2009.
[9] E. Yoneki and J. Bacon. A survey of Wireless Sensor Network technologies: research trends and middleware's role. Technical Report, 2005. http://www.cl.cam.ac.uk/TechReports, ISSN 1476-2986.
[10] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary. Wireless sensor network security - a survey. Security in Distributed, Grid, Mobile, and Pervasive Computing, Auerbach Publications, CRC Press, 2007.
[11] L.L. Fernandes. Introduction to Wireless Sensor Networks Report. University of Trento. 2007, http://dit.unitn.it/~fernand/downloads/iwsn.pdf.
[12] A. T. Zia. A Security Framework for Wireless Sensor Networks. 2008, http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf.
[13] P. Mohanty, S. A. Panigrahi, N. Sarma, and S. S. Satapathy. Security Issues in Wireless Sensor Network Data Gathering Protocols: A Survey. Journal of Theoretical and Applied Information Technology, 2010, pp. 14-27
[14] M.J. Karmel Mary Belinda and C. Suresh Gnana Dhas. A Study of Security in Wireless Sensor Networks. MASAUM Journal of Reviews and Surveys. Sept. 2009, vol. 1, Issue 1, pp. 91-95.
[15] S. Ganeriwal, S. ¢Capkun, C.-C. Han, and M. B. Srivastava. Secure time synchronization service for sensor networks. In WiSe '05: Proceedings of the 4th ACM workshop on Wireless security, pages 97–106, [30]New York, NY, USA, 2005. ACM Press.
[16] J. Newsome, E. Shi, D. Song, and A. Perrig. The Sybil attack in sensor networks: analysis & defenses. In Proceedings of the third international symposium on Information processing in sensor networks, pages 259–268. ACM Press, 2004.
[17] Y. C. Hu, A. Perrig, and D.B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '03), vol. 3, San Francisco, CA, Mar. 2003, pp. 1976-1986.