Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 6, June 2015, pg.871 – 876

RESEARCH ARTICLE

A Study on Security Issues and Sybil Attack in Wireless Sensor Networks

Anil[1], Yashpal Singh[2]

1Research Scholar, Department of Computer Science and Engineering, Ganga Institute Of Technology & Management, Kablana
Email ID: adahiya0007@gmail.com

2Associate Professor, Department of Computer Science and Engineering, Ganga Institute Of Technology & Management, Kablana
Email ID: yashpalsingh009@gmail.com

Abstract: ***Due to broadcast nature of Wireless Sensor Networks and lack of tamper-resistant hardware, security in sensor networks is one of the major issues. Hence research is being done on many security attacks on wireless sensor networks. Sybil attack is a particular harmful attack. When a node illegitimately claims multiple identities or claims fake id, is called Sybil attack. This paper focuses on various security issues, security threats, Sybil attack and various methods to prevent Sybil attack.***

Keyword: Wireless Sensor Networks, Security, Sybil Attack.

1. INTRODUCTION

A wireless sensor network (WSN) is a homogeneous system consisting of spatially distributed autonomous devices that use millions of tiny, inexpensive sensors to monitor physical or environmental conditions. The sensor networks have a wide variety of applications in a number of domains due to the availability of micro-sensors and low-power wireless communications. These sensor nodes will perform significant signal processing, computation, and network self-configuration to achieve scalable, robust and long-lived networks [1]. WSNs is a special class of ad hoc networks that operate with little or no infrastructure and have attracted researchers for its development and many potential civilian and military applications such as environmental monitoring, battlefield surveillance, and homeland security. In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks, which presents a demand for providing security mechanisms in the network [2]. Therefore traditional security techniques in computer networks are not suitable for wireless sensor networks. Researchers have begun focusing on building a sensor trust model to solve the problems beyond the capability of traditional

techniques and they have tried to address the challenges of maximizing the processing capabilities wireless sensor nodes while also securing them against attackers.

WSN ARCHITECTURE

In a basic WSN architecture (fig 1), the many 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 LabVIEW graphical development environment can perform advanced processing and analysis and present your data in a fashion that meets your needs.

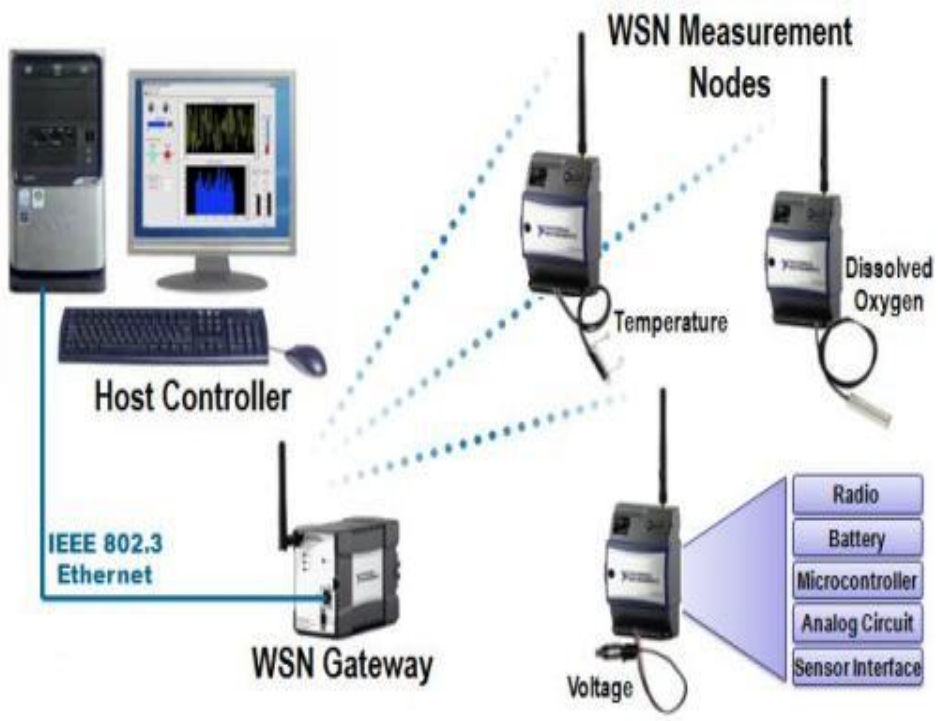

Fig 1: WSN Architecture

2. MODEL USED

Sybil attack is defined as a malicious device illegitimately taking on multiple identities In this thesis, firstly we have implemented the simple form of Sybil attack. Then we have proposed an algorithm to detect the Sybil attack. The proposed algorithm has three phases. The first phase detects the Sybil nodes from the new added nodes in a network which have all trusted nodes. We have used the parameters like packet delivery ratio, number of packets generated and network throughput to prove them the Sybil nodes. The second and third phases are used to give the confirmation that the nodes detected as Sybil nodes in first phase are actually the Sybil nodes. Three scenario of this algorithm has been implemented by number of trust nodes and Sybil nodes in the original algorithm.

2.1 Algorithm Used

The following algorithm has been proposed:

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).

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).

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.

3. Literature

3.1 SYBIL ATTACK

We define the Sybil attack as a malicious device illegitimately taking on multiple identities. We refer to a malicious device's additional identities as Sybil nodes. We propose three orthogonal dimensions: direct vs. indirect communication, fabricated vs. stolen identities, and simultaneity.

3.2 KNOWN THREATS POSED BY SYBIL ATTACK

Distributed Storage: A Sybil attack can defeat replicated storage and redundancy mechanisms in Peer to Peer and sensor networks. Data may be replicated across several nodes (distributed hash table) to achieve redundancy. However due to the presence of a malicious node assuming multiple identities, data may be stored on the identities generated by same node (data may be actually stored on same node).

Multipath Routing: Sensor nodes may use geographic routing to route the data to the base station. In a sensor network, data may be routed through multiple node disjoint paths (multipath routing) to achieve benefits like fault tolerance, increased bandwidth or improved security. However, a malicious node assuming multiple identities can be a part of multiple node disjoint paths which makes multipath routing ineffective .

Data aggregation: In a sensor network, in order to reduce the total number of messages sent and hence save energy, sensor readings from multiple nodes may be processed at aggregation points. By assuming multiple identities, a malicious node may be able to contribute to an aggregate many times. With enough Sybil nodes, an attacker may be able to completely alter an aggregate reading.

Voting: Depending on the number of identities a malicious node assumes, a malicious node may be able to determine the outcome of any vote. A malicious node can either claim that a legitimate node is misbehaving or Sybil nodes can vouch for each other.

Fair-Resource Allocation: A malicious node assuming multiple identities can obtain an unfair share of any resource. Consequently, a malicious node can cause Denial of service to legitimate nodes, and also give an attacker more resources to perform attacks .

Misbehavior Detection: Suppose that the network can potentially detect a particular type of misbehavior. It is likely that any such misbehavior detector has some false positives. As a result, it might not take action until it observes several repeated offenses by the same node. An attacker with many Sybil nodes could "spread the blame", by not having any one Sybil identity misbehave enough for the system to take action. Additionally, if the action taken is to revoke the offending node, the attacker can simply continue using new Sybil identities to misbehave, never getting revoked himself.

4. Major Objectives

In this paper following objectives shall be achieved for efficient delivering of data from source to destination:

1) To study Wireless Sensor Networks.

2) To study various attacks and security mechanisms in WSN.

3) To study and implement Sybil attack in WSN.

4) To study various approaches to prevent Sybil Attack in Wireless Sensor Networks.

5) Analyzing and comparing different approaches.

6) Implementing simple form of Sybil attack.

7) Proposing and implementing an efficient algorithm to detect Sybil attack.

5. Conclusion

In this paper, we presented a concise survey on sensor networks security, security issues and attacks. 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. Then we discussed one of the major attack- Sybil attack and 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. We have also listed notable methods that have been proposed over time to tackle these attacks, their advantages and disadvantages.

References

[1] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[2] Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.

[3] 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.

[4] 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.

[5] L.L. Fernandes ,"Introduction to Wireless Sensor Networks Report", University of Trento. 2007, http://dit.unitn.it/~fernand/downloads/iwsn.pdf

[6] A.T. Zia, "A Security Framework for Wireless Sensor Networks", 2008, http://ses.library.usyd.edu.au/bitstream/2123/ 2258/4/02whole.pdf

[7] 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.

[8] Shio Kumar Singh , M P Singh , and D K Singh "A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011, ISSN: 2231-2803.

[9] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti, **"**A Survey on Wireless Sensor Networks Security", **SETIT 2007** 4th International Conference: **S**ciences of **E**lectronic, **T**echnologies of **I**nformation and **T**elecommunications March 25-29, 2007 – TUNISIA.

[10] 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.

[11] H.K. Kalita and A. Kar, "Wireless Sensor Networks Security Analysis", International Journal of Next-Generation Networks (IJNGN), vol. 1, no. 1, Dec. 2009, pp. 01-09.

[12] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[13] Hemanta Kumar Kalita and Avijit Kar ,"WIRELESS SENSOR NETWORK SECURITY ANALYSIS", International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009.

[14] James Newsome, Elaine Shi. Dawn Song and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", ***ZPSN'O4,*** April 26-27, 2004, Berkeley, California, USA. Copyright 2004 ACM 1-581 13-846-6/04/0004 ... $5.00.

[15] B. N. Levine, C. Shields, and N. B. Margolin, A survey of solutions to the Sybil attack, University of Massachusetts Amherst, Amherst, MA, 2006.

