IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Efficient Defense Mechanishm Against Sybil Attack In Wireless Sensor Network: A Review

Seema[1],Jyoti Kataria[2]

[1]MTech Scholar, [2]Asstt. Professor

[1,2]Department of Computer Science & Engineering MITM Jevra Hisar (Haryana)

Abstract- The sensor consists of small sensors and actuators with common computer objectives for monitoring joint physical and environmental conditions, such as temperature, pressure, etc. Wireless Sensor networks are particularly characterized by limited power structures that can be harvested or maintained, a powerful network topology, large deployments. Sensitive networks have a wide range of performance in the field including residential monitoring, object tracking, retrieval, land slide detection and surveillance. As wireless nerve networks continue to grow, so does the need for effective safety measures. While there are many types of security attacks on WSNs, we have decided to focus on our most critical analysis: Sybil attacks. Sybil's attack is successful when a malicious node, called the Sybil node, illegally seeks multiple identities by naming a new identity or pretending to be an existing one. The purpose of Sybil's attack is to obtain an unparalleled amount of influence over the network through its false identity. Sybil's attack has now posed a serious threat to the wireless network of routing, voting system, proper resource allocation, data integration and discovery of misconduct. There are therefore many suggested ways to detect and prevent Sybil attacks on the wireless network of nerves. A detailed study of these methods has been performed and a comparison table provides an overview of the operation of the method. The conclusions were drawn using a comparison table. The parameters indicate how this method works. Simulation work is done in the NS2 simulator. We used a simple Sybil attack method and an algorithm is proposed to detect Sybil attacks. Performance testing is done using packet delivery rate, the number of packages produced. The results show that the packet delivery rate and the number of packets generated by the same Sybil nodes in each case.

1.1 LIFE TIME

A wireless network is a group of nodes (sensors) that organize a network of networks [1]. Each node contains power processing (one or more microcontrollers, CPUs or DSP chips), which can contain multiple storage types (system, data and flash memory), and an RF transceiver Nodes communicate wirelessly and often organize themselves after the planting of hoc fashion. These tiny sensors have the ability to hear, process data, and communicate with each other. (WSN) relying on the cooperative work of a large number of sensors available. Sensor nodes can be used within multiple deployment environments such as continuous detection, event detection, event identification, location detection, and local control of actuators for a variety of applications such as military, environmental, health, space exploration, and disaster relief. Although a large volume of research is being done and other algorithms are being proposed, there is ongoing research on the subject in recent years [2].One of the most challenging topics and barriers to construction on WSNs is safety. Because the sensors nodes have limited storage and computational resources, they can be easily attacked. Various types of attacks such as wormhole attack, sinkhole attack, selective forward attack, Sybil attack can occur on the network. Dangerous attacks especially on networks sensitive to Sybil attacks as these attacks can put the network at risk of further attacks. Sybil Attack is where a node illegally seeks more ownership. Sybil's attack has now posed a serious threat to the wireless network of routing, voting system, proper resource allocation, data integration and discovery of misconduct. There are therefore many suggested ways to detect and prevent Sybil attacks on the wireless network of nerves.

Wireless Sensor networks are identified by:

- Power Limited power is stored in the harvest.
- Node failure to deal with.
- Areas of Heterogeneity.
- Maximum delivery of.
- Ways to Travel.
- Communication Failure to communicate.
- Top Dynamic network topology.
- Strength to withstand harsh environmental conditions

1.2 WSN STRUCTURE

In the standard WSN architecture (fig1.1), measurement nodes are used to obtain measurements such as temperature, voltage, or even the oxygen produced. Nodes are part of a wireless network-controlled network, which controls network features such as customer authentication and data security. The gate collects measurement data from each node and sends it over a wired connection, usually Ethernet, to the Host controller. There, software such as the NI Lab VIEW graphical development environment can perform advanced processing and analysis and present your information in a way that meets your needs.

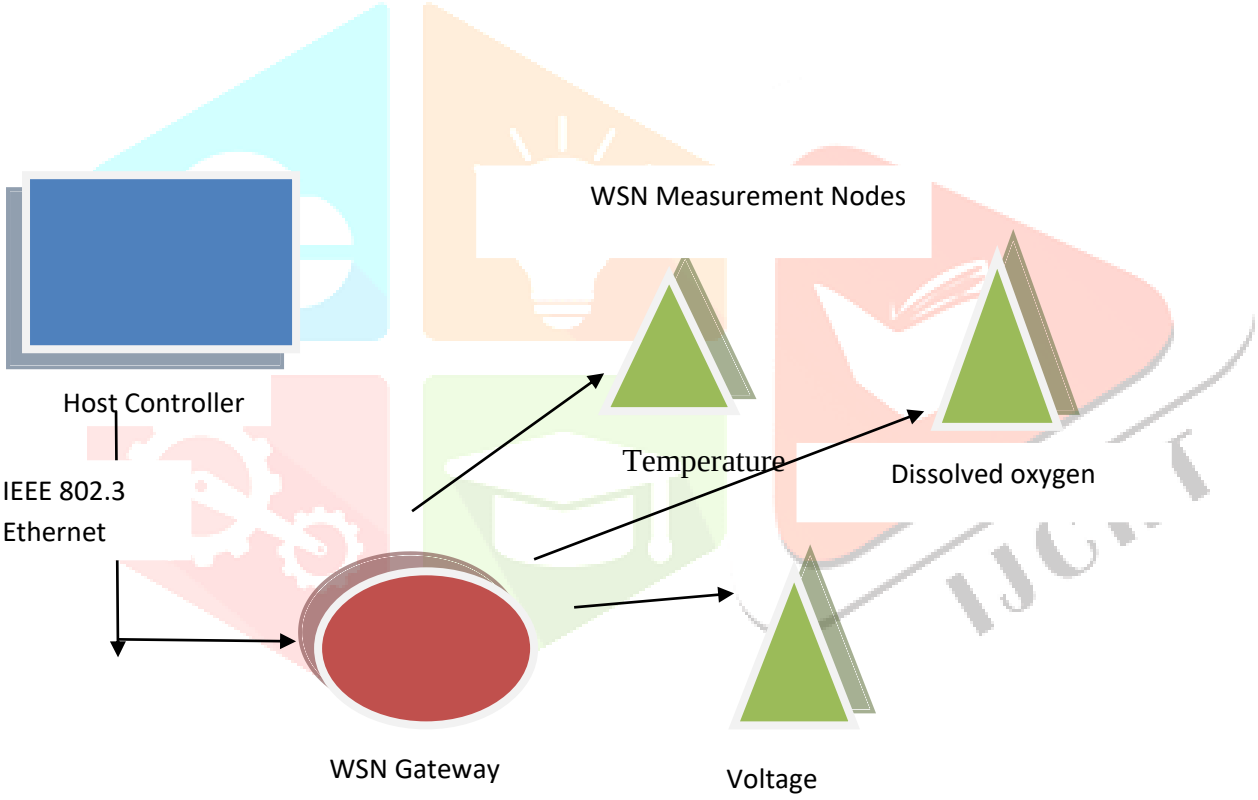

Figure 1.1: Wireless Sensor Network [5]

LITERATURE REVIEW

The following papers are read to explain Sybil's attack literature on wireless nerve networks:

1. Security with wireless nerve networks (Daniel E. Burgner, Luay A. Wahsheh)

The research reviewed in this paper represents the tip of the iceberg when it comes to the safety of wireless nerve networks. Architecture plays an important role in wireless sensor networks as it does with different security issues such as how security affects themes and design issues as well as privacy, integrity, and authenticity. Algorithms also play a role in the process of building a wireless sensor network. Finally, operational issues are discussed to determine whether the proposed project is likely to be implemented. Based on the security analysis of all wireless nerve networks, it is concluded that SOWSN has excellent performance because it is based on real-world conditions. Much research in this area will continue as it is an emerginz technology in the years to come.

2. Protection against Sybil attacks on nerve networks (Qinghua Zhang, Pan Wang, Douglas S. Reeves, Peng Ning)

In Sybil attacks, one node illegally exposes multiple identities to other nodes. This paper suggests how to protect against such attacks on nerve networks. A valid node-to-node authentication protocol uses the key chains of one-way authentication of the message. This method does not require clock synchronization between nodes, and is powerful against human attack in the middle. The extension of this method uses node deployment information to reduce computer overload in each location. This extended method has a significant increase, with a slight decrease in the security it provides.

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

In this paper, they describe Sybil's attack and establish a tax for this attack by separating the different types of attacks. Definition and taxation are very important in understanding and analyzing the threat and protection of Sybil attacks. They introduced a number of novel ways in which a node can verify that other Sybil IDs, including radio resource testing, random key distribution distribution, position verification and registration. The most promising approach among these is the random key distribution that includes the node keys and their identity. Random key distribution will be used in most secure communication situations, and because it depends on well-understood cryptographic principles it is easier to analyze than other methods. These methods are powerful on fixed nodes. In particular, they have shown that in a smart multi-space scheme with a single key holder of 200 keys, the attacker will need to reduce 400 nodes before they have a 5% chance of being able to build new Sybil attack beads.

4.WSN: A report of some researchers

In this chapter they describe four key elements of wireless sensor network security: barriers, requirements, attacks, and protection. Within each category they also categorize the major topics including route, trust, service rejection, and so on. Their purpose is to provide a general overview of the broader area of wireless network security, and to provide key quotes such as that continuous review of relevant documents can be completed by an interested researcher. As wireless nerve networks continue to grow and become more common, they expect more security expectations to be required in these wireless network applications. In particular, the addition of public key encryption and the addition of community-based key management will make solid security a realistic expectation for the future. They also expect that current and future work on privacy and trust will make wireless nerve networks a more attractive option in newer platforms.

5. Detection of sybil attacks on wireless nerve networks (S.Sharmila, G Mother)

Many existing methods for detecting Sybil attacks have been studied and a proposed algorithm for detecting Sybil attacks on a wireless network of sensors. The rate of packet delivery and network packet, before and after acquisition is analyzed by different traffic levels. It is found that the pass rate and package after detection have improved.

6. WSN for protection: Matter and Provocation

They use the Neyman-Pearson detector to locate the sensor location for wireless network sensor networks. To find a way to break, they used Dijkstra's very short route algorithm using the Mthe log negative for chances of missing out as grid point weights. Chances of breaches are defined as missed opportunities of a weak breach. The false alarm level barrier has a significant impact on network access detection performance, which is measured by the probability of breach. The model and results developed here provide indicators that link false alarms and energy efficiency. Forcing a low number of false alarms to avoid unnecessary response costs means a large data set (L) and as a result greater battery consumption, or a solid weight network, which increases shipping costs. The same quality and / or limited considerations regarding the relationship between different parameters can also be made. Wireless nerve networks often fail. In addition, sensor nodes die due to their limited power sources. Therefore, the sensor node failure must be modeled and included in the calculation method for future violations. To simulate network reliability throughout the life of a wireless network sensor is required. Finally, especially in the use of perimeter monitoring, barriers to the environment play a very important role in hearing and should be included in the field model. Integrated data metrics are adopted to select the most experienced subset to participate in the data fusion distribution framework. The function of the senses is to create the right environment and to track objectives. Imitation results show a power saving of 36% of the tracking quality provided can be achieved by selecting co-sensing sensors according to the metrics of the combined information. In all experiments, they assumed that all sensory nodes sent reliable data to a network. In future work, detection of faulty and off-line sensors should be investigated, and precautionary measures should be taken. Consider the effect of sensor selection algorithms in the context of a single tracking data distribution. The presence of multiple targets presents challenges for the tracking organization and the track-to-sensor organization, as well as problems related to access control and routing.

7. Safety audit on safeguarding in case of Sybil attack in WSN

They have tested several types of protections against Sybil attacks on wireless nerve networks using five metrics: durability, interaction, processing complexity, retention difficulty, and communication complexity. In many cases, these metrics alone are not sufficient to determine the usefulness of a particular defense, although it does help to balance trade and asset performance. For example, radio resource testing has appropriate matrix values. However, it is considered unusable due to its need for each location with only one radio. Similarly with code evidence, it requires the attacker to go a long way to build more details in order to carry out the Sybil attack. However, its proposed use now to detect Sybil attacks (e.g. calculation time) is not a very reliable method as many things can contribute to this (e.g. common network delays). On the other hand, local validation has absolute robustness and, in all defenses, it is highly possible to manage the top network networks. However, more advanced communication is required for location verification. In addition each node needs to rely on its viewers; if the Sybil attack is successful, the original Sybil site may lie about the location of other Sybil nodes to prevent detection. Key-based methods seem to be the most suitable for our metrics - ECC is a promising solution for asymmetric key cryptography due to its short key length requirement. In addition, public key verification provides high connectivity and high durability, both of which are highly desirable. Further research in this thesis should show promising results. In the case of smart, fixed key schemes, in order to protect large networks, one must always deal with an important management problem. Most space schemes, including location-based schemes, work best on those large networks but require a number of dense nodes. Similarly, probabilistic models also require dense, uniform networks. In addition, it is very effective in strengthening and connecting. They view polynomial-designed schemes as advanced over matrix-based schemes as they provide the same durability and connectivity, but require less maintenance and less contact.

8. RSSI-based program for Sybil Attack Detection on Wireless Sensor Networks (Murat Demirbas, Youngwhan Song)

They have provided an RSSI-based solution to the problem of Sybil attacks on WSN. They have shown that although RSSI time varies and is generally unreliable and radio transmission is not isotropic, using a range of RSSIs from multiple recipients is possible to overcome these problems. Our protocol is lightweight - alongside recipients who need to work on one node - and solid - they get 100% complete detection and less than a few false points.

9. Network Security Research and Attack Defense Mechanism for Wireless Sensor Networks (Shio Kumar Singh, M P Singh, and D K Singh)

Security becomes a major concern for the wireless sensor network which is restricted due to WSN's wide range of sensitive security systems. Therefore, security on WSNs has attracted a lot of attention in recent years. The key features of WSNs make it a major challenge to design strong protection protocols while maintaining low overheads. In this paper, they have introduced specific security issues, threats, and attacks on WSNs and other solutions. WSN network security remains the most productive indicator in ongoing research.

10. Strategic Review of Sybil Attack (Nitish Balachandran, Sugata Sanyal)

In this paper, they discuss the key types of Sybil attacks that can be implemented on various application domains. They also listed the respected methods proposed over time to deal with these attacks. In addition, they elaborated on their operating methods, benefits, and limitations.

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

This paper analyzes security issues, threats and attacks and the needs of wireless network networks. This paper continues to propose a security framework and security building to integrate existing technology with WSN technology, providing secure and private communications to its users.

12. Wireless Network Network Research (Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti)

This paper presented a summary of research on network issues, security requirements, attacks and security measures. As noted, security requirements are important in protecting the enemy from compromising the security of a distributed wireless radio network. Established protocols and mechanisms for the use of wireless network networks should meet a number of security and operational requirements.

13. Analysis of the wireless nerve network (Hemanta Kumar Kalita and Avijit Kar)

Security in the Wireless Sensor Network is critical to the reception and use of sensor networks. In particular, the Wireless Sensor Network product in the industry will not be accepted unless there is a security of unreasonable evidence on the network. In this paper, they have made a threatening analysis for Wireless. The Sensor Nerve also suggested other forms of resistance. Layer encryption methods and authentication methods may be the first appropriate measurement of external mote-level defenses, but cryptography is not sufficient for self-defense against laptop and internal opponents: careful protocol design is also required.

3. COMPARISON OF DIFFERENT DEFENSE MECHANISMS

Protecting	**Who can work--ate**	**Sybil Disability**	**Disability / Limitations**	**Application Domain**
Trusted Certification	Any	IDs shared	Higher overhead and Cost	General
Radio Service Test	Neighborhood	Indirect com.,Different	It does not work in most programs	Usually
RSSI-based program	Anyone	IDS shared	Does not use existing Sybil nodes in the network, Location calculations are more expensive, Restricted to sensor networks	Sensor Networks
Random key distribution	Anyone key / shared	IDS shared	Restricted to sensory networks	Sensor Networks
Location / Position Verification	Neighbors	Indirectly Com.	Restricted only to wireless advertising networks	Wireless ad networks

Table 1: Comparing different methods of protection

PROMISED TECHNOLOGY

4.1 MOTIVATIONS

In recent years, the wireless sensor network has been widely used in the field of military, health care and forest surveillance etc. It's a hotspot. Because the sensors nodes have limited storage and computational resources, they can be easily attacked. Various types of attacks such as wormhole attack, sinkhole attack, selective forward attack, Sybil attack can occur on the network. Dangerous attacks especially on networks sensitive to Sybil attacks as these attacks can put the network at risk of further attacks. Sybil Attack is where a node illegally seeks more ownership. Sybil's attack has now posed a serious threat to the wireless network of routes, the voting system, the equitable distribution of resources, the consolidation of data, and the discovery of misconduct. There are therefore many suggested ways to detect and prevent Sybil attacks on the wireless network of nerves.

4.2 INTRODUCTION TO THE ALGORITHM

Sybil Attack is defined as a malicious device that illegally owns. In this sense, we first use the simple method of Sybil attack. After that we suggested an algorithm to detect Sybil attacks. The proposed algorithm has three stages. The first stage detects Sybil nodes from new sites added to the network with all trusted nodes. We used parameters such as packet delivery numbers, number of packages produced and network installation to authenticate Sybil nodes. Phases two and three are used to ensure that the nodes identified as Sybil nodes in the first phase are actually Sybil nodes. The third condition of this algorithm is made up of the number of trust nodes and Sybil nodes in the original algorithm.

4.3 ALGORITHM

The following algorithm has been suggested:

Category I:

1. Take another trust node (15).

2. Add a few (5) nodes to the trust node network. These new additional nodes can be Sybil or trust nodes.

3. Transfer data from new nodes to new trust nodes.

4. Calculate the packet delivery rate and the number of packets produced in the given time.

5. Return Sybil locations on the basis of step 4 (Sybil node will have approximately the same amount of packet delivery and the number per packet produced).

Category II:

1. Select remote locations.

2. Phase I Symbols nodes I will transfer data to trust nodes.

3. On the basis of the procedure, find out that the Sybil nodes (Sybil nodes found in the previous section will follow the same method for sending data to any particular node).

Category III:

1. Post packets between new additional Category I locations.

2. Based on the number of hops between the areas, find Sybil locations.

3. If there is no hop between the two nodes, then these will be Sybil nodes.

USE

5.1 NS-2 GRANT

The simulator is focused on the object and is based on two languages: C ++ as a developmental language and Object Tool Command (oTcl) as a simulation language.The ns-2 simulation environment offers great visibility in investigating the features of sensory networks because it already has visible ible models of ad hoc-restricted networks. In the environment of thens-2, a sensory network can be built with many of the same protocols and features as those found in the real world. The network communication environment in ns-2 includes support for individual paradigms and agreements. The wireless model also includes motion support for nodes and power barriers. By using existing network communication infrastructure, we have expanded the ability to simulate sensory networks.

Sensor Network Extensions: The only basic feature of non-ns-2 sensor networks was the concept of something like chemical clouds or moving vehicles that could create sensors close to a channel such as air quality or vibration. Once the sensor has detected a certain “piercing” in that channel, the sensor operates in accordance with the sensor request specified by the ns-2user. This app describes how the sensor will react when it detects an object. For example, the sensor may occasionally send a report to a specific data collection site as long as it continues to detect the practice, or it may do something more complex, such as working with neighboring sensory nodes to detect the object before alerting any external observer. For each sensor network there is a unique sensor app to accomplish diagnostic, such as surveillance, environmental monitoring, etc. With ns-2, we have provided a place to request sensory applications by circumstances. With these sensor applications, we can learn how ground network infrastructure works under a variety of conditions.

Eligibility and Limitations: NS-2 contains both eligibility and limitations when people use it to emulate WSNs. Ideally, for the first time as an unspecified network simulator, NS-2 can support a wide range of contracts across all levels. For example, ad-hoc and specific WSN protocols are provided by NS-2. Second, the open source model saves imitation costs, and online documentation allows users to easily change and improve codes. As NS-2 is originally intended for IP networks but there are some restrictions when you use it to mimic WSNs. First, NS-2 can mimic selected goals but not moral behavior. However, the embedded protocols and applications are intertwined and cannot be firmly separated from the WSNs. Therefore, in this case, the use of NS-2 is incorrect, and it is not possible to get the right results. Second, because NS-2 is designed as a standard network simulator, it does not take into account some of the different features of WSN. For example, NS-2 cannot mimic bandwidth problems, power consumption or energy saving in WSN. Third, NS-2 has a problem growing in WSN, having a problem copying more than 100 sites. As the number of nodes increases, the tracking files will be much larger in management. Finally, it is difficult to add new contracts or parts of nodes due to the structure of NS-2.

5.2 NS2 PLANNING PROCESS

NS2 is a free simulation tool, which can be found at [15]. Works on a variety of platforms including UNIX (or Linux) programs, Windows, and Mac. Developed in the Unix space, without surprises, the NS2 goes well there, as well as its installation. Unless otherwise indicated, Scripture quotations are from the modern-language New World Translation of the Holy Scriptures (UNIX).

NS2 source codes are still distributed in two ways: an all-in-one suite and component-wise. With the package at all, users get all the necessary features and other options. This is actually a recommended choice for beginners. This package provides an “install” script that fixes the NS2 environment and creates a usable NS2 file using the “make” utility.

The current one-in-one suite has the following key features:

• Issue of NS 2.30,

- Release of Tcl / Tk 8.4.13,

• OTcl 1.12 release, once

- The release of TclCL 1.18 and the following are optional:

• NAM Release 1.12: NAM is a animation tool for viewing the network NAM is a animation tool for simulation and notch packet.

• Zlib Type 1.2.3: This is a library required for NAM.

• Xgraph version 12.1: This is a data element with interactive buttons to capture, zoom in, print, and select display options.

The idea of a partly clever way is to find the pieces above and insert each one individually. This option saves a huge amount by downloading.

Following the instructions followed to install ns2.35 in human 12.04:

1. Download NS-23.5

2. Go to the terminal (ctrl + Alt + t) and install the required updates using the command "**sudo apt-get update**".

3. Then enter the required ns2 libraries using the command “sudo apt-get install build-**essential autoconf automake libxmu-dev”** (without limitation)

4. perform the instructions one by one as given below

Cd ns-allinone-2.35

./ to install

cd

sudo apt-get install ns2

Installing NAM

cd ns-allinone-2.35 / nam-1.15 /

5.3 PERFORMANCE OF PERFORMANCE

Here is a program to simulate a simple Sybil attack. The number of sensory nodes taken is small. This program only shows how the packets will be directed to a malicious node while we are trying to export it. The destination node is a malicious node id.

After that we have implemented the proposed algorithm to detect Sybil nodes. We have created three scenarios for this algorithm by changing the number of trust nodes and Sybil nodes.

5.3.1 COMPARATION FEES:

The parameters used in our simulation are shown in following Table . A few nodes are selected and given multiple identities acting as Sybil nodes.

PARAMETER	VALUE
Area	215mX215m
Nodes	20,30,32
Packet Size	2000
Transmission Agreement	UDP
Traffic	CBR Application
Measurement time	30.0 sec
Priqueue line type	Drop Trail/Priqueue
Distribution Model	Two way ground
Antenna Model	Omni antenna
Routing Protocol	AODV
Type of Attack	Sybil Attack

Table 2: Simulation Parameters

5.3.2 MEASUREMENT RESULTS

5.3.2.1 EASY MEASUREMENT OF SILVER ATTACKS

At first only the simplest form of Sybil's attack was included. Here the network is established with 31 nodes. The data transfer from node 0 to node 10, 11 and 20 which are our path node. In one case, there are no attacks, which is why all the data goes to landing points. But in the second case, nodes 10,11 and 20 are fake IDs of node 15, which is why all data will go into 15 instead of 10,11 and 20

CONCLUSION AND FUTURE WORK

In the current report describe various security attacks on wireless nerve networks. After that we focus on some dangerous attack - Sybil Attack. We define Sybil's attacks and create a tax regime with these attacks by separating a different attack font. We describe Sybil's attack as a malicious device that illegally takes over multiple ownership. The definition and tax structure looks very good in identifying and analyzing the protective shields of Sybil's attacks. Dissertate key types of Sybil attacks presented in various application domains. suggested over time to deal with these attacks and we have listed the most important methods. Earlier, we described in detail their methods, benefits and limitations. TABLE 5.1 summarizes this. After that we use a simple Sybil attack method using NS2 to show how Sybil attacks work on a small network. We developed an algorithm to detect Sybil attacks. This algorithm has three stages. the first phase finds Sybil nodes and the second and third phase provides confirmation of Sybil nodes. Network transmission increases when there are 30 nodes and 2 sybil nodes compared to the situation where there are 20 nodes and 2 sybil nodes.In the future, the work can be done using different conditions and limitations. Ways to increase network access can be created. Improvements to this approach can also be made by developing Sybil node termination strategies.

REFERENCES

[1] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister. System Architecture Directions forNetworked 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 ComputerScience 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 ofNetworks, 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.