Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 4 (2017), pp. 531-538

http://www.ripublication.com

Enhancing Security of WSN Using AIS

Dr. Nipin Gupta[1], Dr. Pankaj Gupta[2], Deepak Goyal[3], Monika Goyal[4], Swati Phogat[5]

[1] Associate Professor ECE, Vaish College of Engineering, Rohtak, Haryana, India.
[2]Professor, CSE, Vaish College of Engineering, Rohtak, Haryana, India.
[3]Associate Professor, CSE, Vaish College of Engineering, Rohtak, Haryana, India.
[4] Assistant Professor, Vaish Mahila Mahavithyla, Rohtak, Haryana, India.
[5]M.Tech student, Vaish College of Engineering, Rohtak, Haryana, India.

Abstract

Wireless Sensor networks (WSN) is an emanated technology and have variety of applications areas such as battlefields, in buildings, for traffic surveillance, for habitat monitoring, in automation, fire detection system, smart homes, remote patient health monitoring system etc with huge impact on technology enhancement. One of the bothering challenges that wireless sensor networks usually face today is security of network. As the deployment of sensor nodes in an unattended environment makes the wireless networks vulnerable to a variety of attacks, the power limitation and low memory of sensor nodes also makes conventional security solutions unfeasible. The wireless communication technology acquires various types of security threats. Thus security has become the forefront of network management and implementation. There are many attacks which makes the network inefficient such as sybil attack. This paper discuss the method to enhance the security of network using Artificial Immune System. The organic immune system is a vigorous, complex, adaptive system that defends the body from distant pathogens. It is able to categorize all cells (or molecules) within the body as self-cells or non-self cells. The resistant algorithm applied to the model is the clonal choice algorithm. The proposed algorithm removes the Sybil attack in the WSN.

Keywords: Wireless Sensor Network, Sybil attack, Artificial Immune System, Clonal selection mechanism.

INTRODUCTION

WSN consists of a number of small, cheap, disposable sensor nodes that perform certain functions. Wireless sensor network applications include wildlife monitoring, bushfire, military command, intelligent communications, industrial quality control, observation of critical infrastructures, smart buildings, distributed robotics, traffic monitoring, examining human heart rates etc. Majority of the sensor network are expanded in hostile environments with active intelligent resistance. Therefore security is a crucial issue and one useful example

of its application is in battlefield in which there is a pressing need for secrecy of location, messages, resistance to subversion and destruction of the network. The security goals are classified as crucial and derived. The primary goals are also known as standard security goals such as Confidentiality, Integrity, Authentication and Availability (CIAA). The derived goals are Data brightness, Self-Organization, Time management and Secure Localization. [1] Wireless Sensor networks are open to to security attacks due to the transmit nature of the communication intermediate. Furthermore, wireless sensor networks have extra vulnerability because nodes are often placed in a dangerous environment where they are not physically protected. Basically attacks are classified as shown in the Figure1. The security mechanisms are basically used to detect, prevent and recover from the security attacks. A wide variety of security schemes can be invented to control malicious attacks and these can be categorized into two types such as high and low-level. Low-level safety measures primitives may consist of key concern and trust setup, secrecy and authentication, isolation, strength to communicate denial of service secure routing etc. High-level security mechanism includes secure group management, intrusion detection, and secure data aggregation.

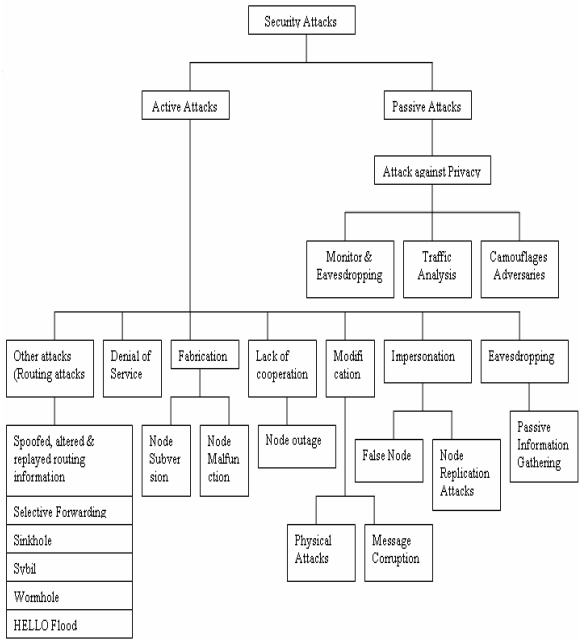

Figure 1. Classifictation of attacks

ARTIFICIAL IMMUNE SYSTEM

Artificial Immune Systems (AIS) are computational models that belong to the computational intellect people and are inspired by the organic resistant structure. During the past decade, they have attracted a lot of researchers aiming to develop immune-based models and techniques to solve complex computational and engineering problems. The crucial job of a organic resistant structure is to protect the body from distant molecules known as antigens. It has great model recognition means that may be used to tell apart among foreign cells entering the body (non-self or antigen) and the body cells (self). resistant structure have many

uniqueness such as uniqueness, self-sufficient, recognition of foreigners, spread detection, and sound patience (Castro and Zuben , 1999).[2]

Given that our own life depends on our immune system, so it is obvious to consider it as one of the most important biological mechanisms that human being possess. In recent years, several researchers have developed computational models of the immune system that attempted to capture some of its most remarkable features such as its self-organizing capability.[4] The organic resistant structure is a robust, compound, adaptive system that defends the body from foreign pathogens. It has the capacity to categorize all cells or molecules within the body as self or non-self cells. This is done with the help of a distributed task force that has the intelligence to take action from a local as well as a global perspective using its network of chemical messengers for communication. There are two main twigs of the resistant structure: native and adaptive immunity. The innate immune system is an unchanging mechanism that detects and destroys certain invading organisms, while the adaptive immune system responds to previously unknown foreign cells and builds a response to them that can remain in body over a long period of time [3]. From the last few years, the AIS has gained much popularity and become important topic of Artificial Intelligence, followed by Fuzzy Logic, Neuro Network and Genetic Algorithm.
The clonal selection principle of AIS describes how the immune cells eliminate a foreign antigen and is efficient approximation algorithm for achieving optimum solution. The basic algorithm is first applied by Charsto et al., for solving optimization problems the steps involved are:

Step 1: Initialize a number of antibodies or say immune cells which represent initial population size.

Step 2: When an antigen or pathogen occupy the organism, a number of antibodies that know these antigens stay alive.

Step 3: The immune cells recognize antigens undergo cellular reproduction. During reproduction the somatic cells reproduce in an asexual form that there is no crossover of genetic material during cell mitosis. The new cells are copies or clones of their parents.

Step 4: A portion of cloned cells undergo a mutation mechanism which is known as somatic hyper mutation.

Step 5: The consideration of every cell with each other is a calculate of similarity between them. It is designed by the coldness between the two cells. The antibodies there in a memory response are going on a higher affinity than those of early crucial response. This fact is referred to as maturation of resistant comeback. During the mutation process the strength as well as the sympathy of the antibodies gets altered. In each iteration after cloning and mutation those antibodies which have higher fitness and affinity are allowed to enter the pool of efficient cells. Those cells with squat affinity or self-reactive receptors must be efficiently removed.

Step 6: At each iteration among the efficient immune cells some become effecter cells or plasma cell, while others are maintained as memory cells. The effecter cells secrete antibodies and memory cells having longer span of life so as to act faster or more effectively in future when in future when the organism is exposed to same or similar pathogen.

Step 7: The process continues till he termination condition is satisfied else steps 2 to 7 are repeated.

Following table represents different parameter of immune system mapped with the network parameter of the WSN.

AIS	WSN
Immune system	Network parameter
Antibodies	Detectors
Antigens	Malicious node
Self	Normal activity
Non-self	Abnormal activity

Sybil Attack

When a node illegitimately claims multiple identities or claims fake IDs, the WSN suffers from an attack called Sybil attack. The node imitates itself to make several copies to baffle and collapse the system. The structure can be attacked upon internally or externally. Exterior attacks can be prohibited by verification but not the interior attacks. There should be one to one mapping between uniqueness and unit in WSN. But this attack disobey this one-to-one mapping by making multiple uniqueness.[5]

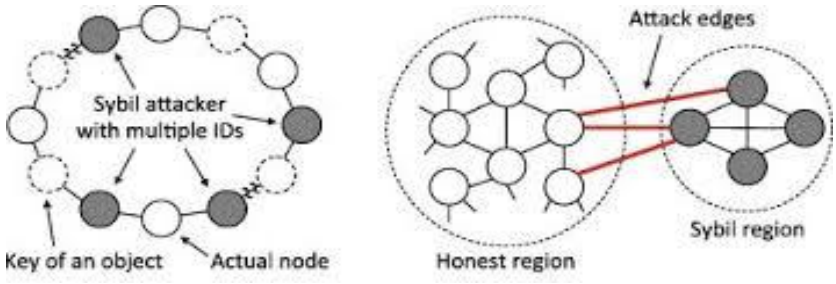

Figure 2. Sybil attack

Types of Sybil Attack

In order to detect the Sybil attack it is necessary to first understand the different ways in which the network can be attacked [6].

(a) Direct and Indirect Communication:

In direct attack, the valid nodes correspond directly with Sybil nodes whereas in indirect attack, the communication is done during nasty node.

(b) Fabricated and stolen identities:

It make a new uniqueness for itself based on the uniqueness of the valid nodes, that is, if valid nodes have an ID with length 32 bit integer, it randomly creates ID of 32 bit integer. These nodes have fictitious uniqueness.

In stolen uniqueness, enemy identifies valid uniqueness and then uses it. The attack may go unidentified if the node whose identity has been stolen is destroyed. Uniqueness duplication is when the equivalent uniqueness are used several times in the identical places.

(c) Simultaneous and non-simultaneous attack:
In simultaneous attacks, all the Sybil identities participate in the network at the same time. While only single uniqueness emerges at a time, basically cycling through uniqueness will build it immediately.
The amount of uniqueness the attacker utilizes is equal to the number of corporal devices; each tool presents different uniqueness at unusual times.

Clonal Selection mechanism
The Clonal Selection Principle describes the basic features of an immune response to an antigenic stimulus. It creates the plan that only those cells that distinguish the antigen proliferate, thus being selected beside those that do not. [7]The main features of the clonal selection theory are that:

- The new cells are copies of their parents known as clones which are subjected to a mutation mechanism with high rates (somatic hyper mutation).
- Elimination of newly differentiated lymphocytes is done that carry self-reactive receptors
- Proliferation and differentiation on contact with antigens of mature cells.
- Elimination of self antigens
- Restriction of one pattern to one differentiated cell and retention of that pattern by clonal descendants.
- Creation of new casual genetic alters subsequently expressed as dissimilar antibody patterns by a form of speed up somatic mutation.

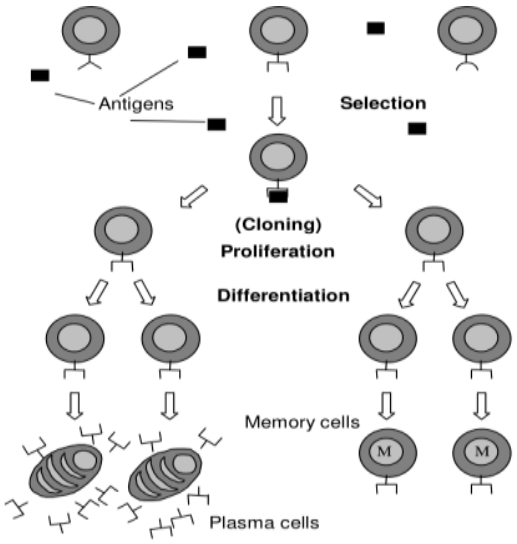

Figure 3. Clonal selection principle

PROPOSED WORK
Sybil attack is a type of attack that is found on network layer and is detected and removed from the network using the model named as Immune Collusion Hull model. The network layer is third layer of OSI model of computer networking and is responsible for packet forwarding including routing through intermediate routers, whereas datalink layer is responsible for media access control, flow control and error checking. It is a practical

structure, the role of which is to organize similar resistant bodies. The ICHM is made up of IB (immune body) and IC (immune channel).
ICH = {Ibi, IC | i belongs to N}, N is the set of natural numbers means ICHM consist of several Ibs and the quantity is user distinct. IB is an integral resistant structure which is fit in network equipment.

The proposed work is carried out at MATLAB which is an abbreviated form of matrix laboratory. It integrates computation, visualization and is a modern programming language environment. It has complicated data arrangement contain built-in editing and debugging apparatus and supports object oriented programming. These factors make MATLAB an excellent tool for teaching and research. The basic data element is of this is an array that does not require dimensioning. The proposed algorithm model when applied to detect and remove Sybil attack the following results are shown.

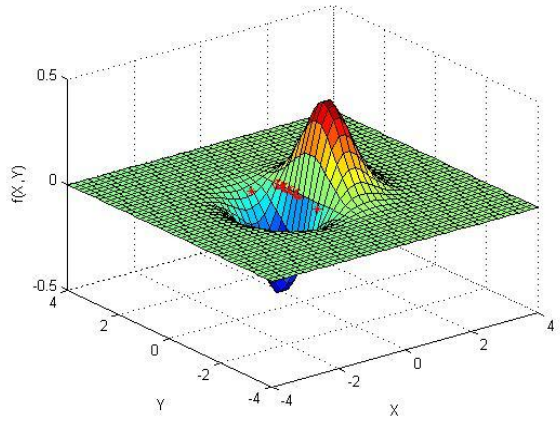

Figure 4. Defected nodes are selected

Defected nodes act as the antigen and thus they removed with the help of proposed model as shown in the figure. Thus packet delivery ratio is also improved as sybil attack is reduced.

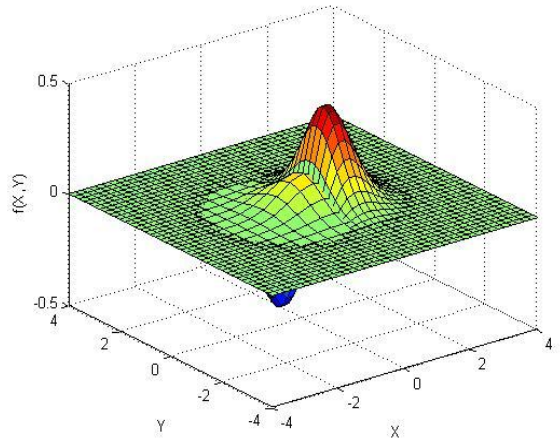

Figure 5. Defected nodes are removed

The Objective function is minimized by using the number of iteration and the plot shows the result. Also the elapsed time is reduced after prevention of attack.

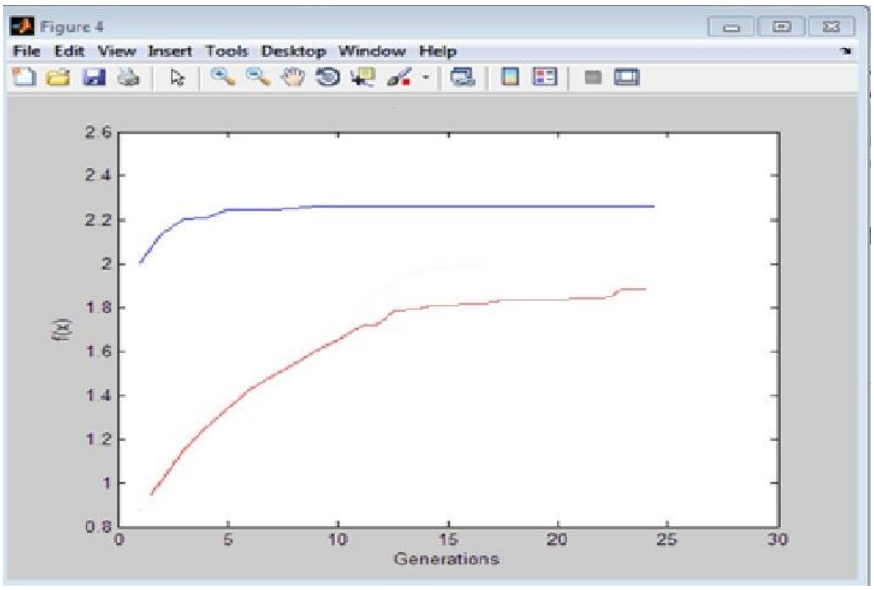

Figure 6. Fitness function

CONCLUSION

Wireless Sensor Networks have emerged as an important application area resulting from the advancement of efficient short-range radio communication and miniaturization of computing devices. Sensor networks are a promising new skills to allow inexpensively feasible solutions to a variety of applications, for example pollution sensing, structural integrity monitoring, and traffic monitoring.[8] One of the chief challenge wireless sensor networks features today is security. Thus in this paper we have proposed a model using artificial immune system which is a relatively novel and promising paradigm to solve the problem of security in WSN. Further this can be used for detecting other attacks on other layers.

REFERENCES

[1] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" *IJCSIS Vol. 4, No. 1 & 2, 2009*

[2] J.R. Al-Enezi, M.F. Abbod & S. Alsharhan "ARTIFICIAL IMMUNE SYSTEMS – MODELS, ALGORITHMS AND APPLICATIONS" IJRRAS 3 (2) May 2010

[3] Dasgupta, D. "Artificial Neural Networks and Artificial Immune Systems: Similarities and Differences", Proc. of the IEEE SMC, 1, pp. 873-878, 1997

[4] Carlos A. Coello Coello, Nareli Cruz Cortes, "Solving Multiobjective Optimization Problems Using an Artificial Immune System" Genetic Programming and Evolvable Machines, 6, 163–190, 2005 Springer Science

[5] S.Sharmila, G Umamaheswari, "DETECTION OF SYBIL ATTACK IN MOBILE WIRELESS SENSOR NETWORKS" [IJESAT] Volume-2, Issue-2, 256 – 262

[6] J. Newsome, E. Shi, and D. Song, "The Sybil Attack in Sensor Network: Analysis & Defences," The Third Intl. Symposium on Information Processing in Sensor Networks (IPSN'04), Berkeley, California, USA: ACN Press, 2004, pp.185-191.

[7] D. Dasgupta, Z. Ji, F. González, "Artificial Immune System (AIS) Research in the Last Five Years"

[8] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses"