

Design Proposed Algorithm to Detect Sybil Attack and Recovery by using Clonal Selection Principle in Immune Collaborative Model

Tarun¹ and Deepak Goyal²

¹M. Tech. Student, VCE Rohtak, Haryana (India)

tarunsangwan662@gmail.com

²Associate Professor and HOD, CSE Department, VCE, Rohtak, Haryana (India)

deepakgoyal.vce@gmail.com

Publishing Date: June 23, 2016

Abstract

This paper is based design a such kind of algorithm that are used to detect Sybil attack and recovery of data by using clonal selection principle, which will very effective role in WSNs which are used in numerous applications such as environmental monitoring, habitat monitoring, prediction and detection of natural calamities, medical monitoring and structural health monitoring. WSNs consist of a large number of small, inexpensive, disposable and autonomous sensor nodes that are generally deployed in an ad hoc manner in vast geographical areas for remote operations. Sensor nodes are severely constrained in terms of storage resources, computational capabilities, communication bandwidth and power supply. The proposed model can detect the Sybil node and recover it effectively.

Keywords: *Immune Collaborative Model, WSN, Security Challenges, Sybil Attack, Clonal selection principle.*

1. Introduction

The Sybil attack is one of the most severe attacks in Mobile Ad hoc Network (MANET) and Wireless Sensor Network (WSN). When a malicious node illegitimately uses multiple phony identities to confuse and collapse the network, we term it as Sybil attack. Sybil attack may happen in a system internally or externally.

External attacks, where the Sybil node is an outsider and tries to enter into the network by some means, can be prevented by authentication mechanism, but it cannot countermeasure internal attacks.

Authentication mechanism ensures that there should be one to one mapping between entity and identity in the network to enable each node to prove itself of not being compromised. But this attack also violates this one-to-one correspondence by generating multiple falsified identities of the same node. Sybil attack spreads excessive hazard in routing protocols, online voting system, fair resource allocation, data aggregation and misbehavior detection system. This attack also corrupts large-scale peer-to-peer systems in which a chance of security threats appears from faulty remote elements. Normally, Peer-to-peer systems rely on the existence of multiple, independent remote entities which can replicate computational or storage tasks (to preserve integrity of data) or distribute tasks among them (to protect against data leakage). So, this type of system must ensure that each entity has distinct identity. Otherwise, a single faulty entity may represent multiple Sybil identities and get control over a considerable portion of the network there by destabilizing the redundancy. In Sybil attack, the adversary targets the victim system by using its Sybil identities and continues attack in order to interrupt that system. For example, a rival can pollute the voting scheme of a reputation system, weaken the routing and data replication services in distributed hash tables (DHTs), or cripple many critical functions of a wireless sensor network such as routing; resource allocation etc. The performance of a reputation system degrades if Sybil identities are generated effortlessly. If the reputation system

accepts inputs from unreliable entities, then linking them to a trusted entity may cause threat for the system. This attack particularly affects decentralized systems, where it is almost impossible to rely on a single authority to certify genuine nodes. However, J. R. Douceur has shown that without a logically centralized authority, Sybil attacks are always possible (i.e. may remain undetected) except under extreme and unrealistic assumption of resource parity and coordination among entities. Since the Sybil attacker can create many fake identities, it thus can increase the probability that the malicious node is selected by other nodes as part of their routing paths. Besides, the Sybil attack can significantly reduce the effectiveness of fault-tolerance schemes such as multi-path routing because other nodes will treat the forged nodes generated by the spiteful node as different nodes and establish different routes through that malicious node. A Sybil attacker may also satire nodes in geographic routing protocol, such as the GRID routing protocol.

In the present scenario of ad hoc network it is a great challenge to prevent and detect Sybil attack as well as to recover the victim network. The subsequent sections of this paper discusses a general framework for countermeasures against the impact of Sybil attack in wireless ad hoc network and different approaches towards innovative detection techniques to mitigate its severe effects. All these countermeasures have been categorized on the basis of Sybil attack prevention, detection and recovery methods which are useful for future researchers to select the proper domain on Sybil attack defense.

A Wireless sensor network is a network of distributed autonomous devices that can sense or monitor physical or environmental conditions cooperatively. Typically, sensor nodes are grouped in clusters, and each cluster has a node that acts as the cluster head. All nodes forward their sensor data to the cluster head, which in turn routes it to a specialized node called sink node (or base station) through a multi-hop wireless communication.

Sensors must be deployed before they can provide useful data. Therefore the deployment of sensors is an important basis for sensor networking. One of the important criteria for being able to deploy an efficient

sensor network is to find optimal node deployment strategies and efficient topology control techniques.

2. Security Challenge in WSN

Security has become a challenge in wireless sensor networks. Low capabilities of devices, in terms of computational power and energy consumption, make difficult using traditional security protocols. Two main problems related to security protocols arise. Firstly, the overload that security protocols introduce in messages should be reduced at a minimum; every bit the sensor sends consumes energy and, consequently, reduces the life of the device.

Secondly, low computational power implies that special cryptographic algorithms that require less powerful processors need to be used. The combination of both problems leads us to a situation where new approaches or solutions to security protocols need to be considered. Wireless links in WSNs are susceptible to eavesdropping, impersonating, message distorting etc. Poorly protected nodes that move into hostile environments can be easily compromised. Administration becomes more difficult due to dynamic topology. Various security challenges in wireless sensor networks are analyzed and key issues that need to be resolved for achieving adequate security are summarized in.

Types of routing attacks and their countermeasures are presented in [6]. A review of security threats to WSNs and a survey of defense mechanisms is presented. In order to design a secure sensor network, several aspects have to be considered [8]: Key establishment and trust setup, secrecy and authentication, and privacy. Key establishment can be considered the base of the system; a secure and efficient key distribution mechanism is needed for large scale sensor networks. Once every node has its own keys, these are used to authenticate and encrypt (if needed) the messages they exchange.

2.1 Sybil attack

When any node creates multiple copies of itself to create confusion in the WSN network or illegally claims multiple identities or claims fake ID'S and also can cause collapse in the network then that kind

of situation can be referred as Sybil system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in WSN network, this Sybil attack violates it by creating multiple identities [9].

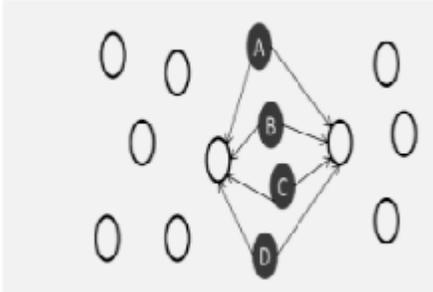


Figure1: Sybil Attack

As it is shown in figure nodes A, B, C and D are Sybil nodes and they can communicate with any of the neighboring nodes and have multiple identities and thus confuse and collapse the network.

2.2 Types of Sybil attack

There are different types of Sybil attack as mentioned below [10]:

2.2.1 Direct and Indirect Communication

In direct communication the communication is between the legal node and the Sybil indirect communication it is between the legal node and the copy of the Sybil node.

2.2.2 Stolen and Fabricated Identities

Stolen identity is that identity which the malicious node takes from the legitimate node and attack. This kind of cannot be identified and find if the legitimate node is destroyed. While fabricated identities are that identities that the copy node or the malicious node takes from the legitimate node or we can say uses the exact same identity as that of the legitimate node. This is known as identity replication attack. This system and n node while in tity uses of in which same identity is used many times in a same network.

2.2.3 Simultaneous and Attack

In simultaneous attack, all the copy nodes or the Sybil identities participate at the same time, but since they have only one identity so this simultaneous attack is supported by the cycling of identities between all nodes. Non-simultaneous is the attacker uses the same number of the identities equal to number of devices.

2.3 Sybil Attacks on Protocols

In Sybil attack, as the malicious code can generate and uses a number of identities on single device than that can create an illusion as if there are a number of legitimate nodes and thus can protocols.

2.3.1 Distributed Storage

As the Sybil attack creates replicated data can be stored in several nodes and thus affect the architecture.

2.3.2 Routing

As one node can be present in a number of routes because of having same identity to a n malicious nodes, routing mechanism is affected.

2.3.3 Data Aggregation

As Sybil nodes contribute many times posing as a number of different users, the aggregated data changes completely, as the data is grouped completely into one node and thus false information occurs.

2.3.4 Voting

As the decisions in the WSN are voting, so the Sybil node can vote many times from the malicious nodes and thus destroyed the process.

2.3.5 Misbehavior Detection

Detecting accuracy of the malicious node is reduced as the Sybil node uses its virtual identities to increase its credit trust vales and reputation.

2.3.6 Fair resource Allocation

Because of the multiple identities, Sybil node affects the allocation of the resource as it have virtual identities, it can obtain an unfair share of resources.

3. Artificial Immune System

The Biological Immune System (BIS) is the one of the most complicated structure and peculiar function system in biological bodies. It is composed of organs, tissues, cells and molecules with immune function. The main action of BIS is to recognize the body's own cells (self) and antigens (non-self), and exclude non-self. The further researches of BIS showed that the performing process of biological immune contains the powerful information processing capabilities, such as recognition, learning, memory, diversity, fault tolerance, distributed detection and so on. Recently, these characteristics of BIS have drawn significant attention. Numerous scholars have come to imitate the mechanism of BIS to apply it to the other fields. All these artificial intelligent system, inspired by immune system, are called the Artificial Immune System (AIS) [11, 12].

Artificial Immune System (AIS) is a framework based upon a set of general-purpose algorithms and models to create abstract components of the immune system. The diversity and self-adaptive characteristics of AIS make it remarkable in anomaly detection. Especially it has the ability to detect unknown intrusions. By simulating the biological immunity, the AIS can offer much evolutionary learning mechanism, such as unsupervised learning, self-organizing, memory etc, and it draws the advantages of Classifier, Neuro-Network and Machine Reasoning, therefore it is considered a great potential to solve problems with new ideas and methods, which maybe can be applied to control theory and control engineering. The research results of AIS relate to cybernation, pattern recognition, fault diagnosis, information Security, intelligent optimizing, machine learning, robotology, data analysis as well as other fields. In the last ten years, the AIS is gaining popularity, and has become another hot topic of Artificial Intelligence, following after Fuzzy Logic, Neuro Network and Gene Algorithm.

4. Mapping of Immune System with Network

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

Immune System	Network Parameter
Antibodies	Detectors
Antigens	Malicious Node
Self	Normal Activity
Non-self	Abnormal Activity

Figure2: Immune System and N/w Parameters

5. Architecture of Immune Collaborative Body

The weak points of AIS prevent it from presenting efficient protection. On the other hand, if the Artificial Immune Systems in WSN with similar environments share their lymphocytes, the conflict between efficiency of AIS. Such a model for lymphocytes sharing is called Collaborative Artificial Immune System, and it is implemented by the structure called Immune Collaborative Body. In order to keep the diversity of immune system, Immune Bodies can join an Immune Collaborative Bodies freely, and only some efficient memory lymphocytes can be shared. It is a virtual system the function of which is to organize similar immune bodies. The ICB is made up of IB (immune body) and IC (immune channel).

$ICB = \{IB_i, IC \mid I \in N\}$, N is the set of natural numbers, that is to say, ICB include several IBs and the amount is user defined. IB is an integral immune system which is installed in network equipment.

5.1 Modules of Immune Body

There are five typical modules in IB, Collaborative module, Immune algorithm, Collaborative Detector Lib, Memory Detector Lib, Mature Detector Lib. Functions of these modules are:

5.1.1 Collaborative Module

Send and receive collaborative detectors, maintain the information of ICB, decide which collaboration to join in and when to quit.

5.1.2 Immune Algorithm

The function of this module is to run immune algorithms, such as negative selection algorithm, clonal selection algorithm and so on. Mature detectors are generated from these algorithms. The clonal selection algorithm is applied on the proposed model.

5.1.3 Mature Detector Lib

Store mature detectors generated by immune algorithms.

5.1.4 Memory Detector Lib

Efficient mature detectors are stored as memory detectors in this lib with longer life circle.

5.1.5 Collaborative Detector Lib

Efficient memory detectors are selected as collaborative detectors and spread to the whole ICB.

5.2 Function of Immune Collaborative Model for WSN

Collaborative module is the main part of the immune body. In order to find out the immune bodies similar with oneself necessary information is stored in the module such as:

5.2.1 Immune Body IP

In order to sign an immune body uniquely.

5.2.2 Immune Body Characteristics

In order to compare with each other to select the similar ones, various characteristics included are node type, coverage area, packet size, initial energy, energy consumed, and residual energy.

- i) Node type will be 1, 2, 3 as the network consists of 3 type of nodes.
- ii) Coverage area: Coverage area of different type of node is different. This property will include coverage area of node.
- iii) Packet size: It gives size of packet to be transmitted.
- iv) Initial energy: It gives initial energy of the node.

v) Energy consumed: It gives the total energy consumed by the node.

vi) Residual energy: It gives the remaining energy of the node. If the remaining energy is 0 then the node is dead.

5.2.3 ICB ID

It is used to sign ICB the immune body belongs to, uniquely.

5.2.4 ICB Characteristics

In order to be compared by other immune body to decide whether to join this ICB or not, these characteristics are:

- i) Number of nodes: It gives the number of nodes in the ICB.
- ii) Head node id: It tells about the id of the head node of the ICB.
- iii) Head node residual energy: specifies the residual energy of the head node after joining immune body to the ICB.
- iv) Threshold energy: It gives the maximum level of the energy of any node.
- v) Threshold delay: It defines the threshold delay in every node in the ICB.
- vi) Max size: It specifies the limit of the maximum size or the maximum number of nodes an ICB can have.

5.2.5 Search criteria

When an immune body wants to join an ICB, it will compare ICB characteristics with its own immune body characteristics based on the search criteria and also can be set by the users.

5.2.6 Exit Rule

Prescribe the condition to exit an ICB.

IB-ID		
IB-characteristic		
Node type	Coverage area	Packet size
Initial energy	Energy consumed	Residual energy
ICB-ID		
ICB-characteristic		
Number of nodes	Head node id	Head node residual energy
Threshold energy	Threshold delay	Max size
Search criteria		
Exit Rule		

2

Figure 3: ICB model for WSN

6. Algorithm of Collaboration

Algorithm of collaboration includes 3 phases, join in collaborative body, collaboration, and quit collaborative body.

1. Join in collaborative body

1.1. New entrant side

1.1.1. Broadcast the Search

Criteria

1.1.2. if (number of ICB satisfy the Search Criteria \geq 1) then:

1.1.3. Choose qualified ICB randomly

1.1.4. Modify the

ICB.ID=chosen ICB.ID

1.1.5. Insert this. IB.IP in contribution table

1.1.6. broadcast ICB.ID

1.1.7. end/

1.1.8. else if(no of ICB satisfy the Search Criteria $<$ 1) then:

1.1.9. ICB.ID=this.IB.IP+this.time // build a new ICB

1.1.10. Insert this.IB.IP in contribution table

1.1.11. broadcast ICB.ID

1.1.12. end

1.2. Other IBs of the ICB

1.2.1. BEGIN

1.2.2. receive broadcast Search Criteria

1.2.3. if(this.ICB.characteristics==Search Criteria)

1.2.4. Insert source.IB.IP in contribution table

1.2.5. else

1.2.6. discarded broadcast package

1.2.7. END

2. Collaboration

2.1. Be helped side

2.1.1. int k //successfully detect, the lifecircle of detector +k

2.1.2. int h //unsuccessfully detect, the lifecircle of detector -k

2.1.3. receive broadcast CD

2.1.4. insert detector in Collaborative Detector Lib

2.1.5. while(amount of nodes in

collaborative model \leq threshold) then:

2.1.6. if(collaborative detector matches antigen) then:

2.1.7. this.CD.lifecircle=this.CD.lifecircle+k

2.1.8. this.CD.contribution=value++

2.1.9. reply sender "ok"

2.1.10. end// CD is a structure of Collaborative Detector

2.1.11. else

2.1.12. this.CD.lifecircle=this.CD.lifecircle -h;

2.2. helping side

2.2.1. while(no of nodes in memory \leq threshold)

2.2.2. Repeat

2.2.3.

if(memory_detector.lifecircle $>$ threshold delay)

2.2.4. memory detector becomes CD

2.2.5. broadcast CD

2.2.6. end

2.2.7. if(received "ok")

2.2.8.

this.CD.contribution_value

++

2.2.9. END

3.1. Exiting side

3.1.1. int sum= Σ Contribution values

3.1.2. if(sum $<$ 1) then:

3.1.3. delete ICB.ID

3.1.4. broadcast exit ICB.ID

3.2. Other IBs of the ICB

3.2.1. received broadcast

3.2.2. delete IB.IP

7. Proposed Algorithm

The proposed algorithm applies the Sybil attack detection and recovery using the proposed immune collaborative model. The Network consists of 20 nodes and Network is heterogeneous and 3 types of nodes are available in network. The whole process can be explained by the following algorithm:

1. Select the source and destination.
2. Apply immune collaborative model on the network and the immune algorithm is clonal selection algorithm.
3. The algorithm replicates the node identities and different IB joins and exits different ICB.
4. Transmit data from source towards destination.
5. While(data doesn't received by the destination)
6. Repeat
7. Different IB joins and exit ICB
8. If(IB-ID is not unique)
9. Then Sybil attack detected.
10. IB characteristics are modified and IB exists from ICB.
11. End if
12. End while
13. Exit

It.: 7 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.48 f(x,y): 2.241
 It.: 8 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.53 f(x,y): 2.245
 It.: 9 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.58 f(x,y): 2.246
 It.: 10 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.63 f(x,y): 2.256
 It.: 11 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.70 f(x,y): 2.256
 It.: 12 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.75 f(x,y): 2.256
 It.: 13 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.78 f(x,y): 2.256
 It.: 14 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.82 f(x,y): 2.257
 It.: 15 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.82 f(x,y): 2.257
 It.: 16 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.85 f(x,y): 2.260
 It.: 17 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.88 f(x,y): 2.260
 It.: 18 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.89 f(x,y): 2.260
 It.: 19 pm: 0.0100 x: 0.62 y: 0.63 Av.: 1.92 f(x,y): 2.260
 It.: 20 pm: 0.0100 x: 0.62 y: 0.63 Av.: 1.93 f(x,y): 2.260
 It.: 21 pm: 0.0100 x: 0.62 y: 0.63 Av.: 1.97 f(x,y): 2.260
 It.: 22 pm: 0.0100 x: 0.62 y: 0.63 Av.: 1.97 f(x,y): 2.260
 It.: 23 pm: 0.0100 x: 0.62 y: 0.63 Av.: 1.99 f(x,y): 2.260
 It.: 24 pm: 0.0100 x: 0.62 y: 0.63 Av.: 2.01 f(x,y): 2.260
 It.: 25 pm: 0.0080 x: 0.62 y: 0.63 Av.: 2.04 f(x,y): 2.260
 It.: 26 pm: 0.0080 x: 0.62 y: 0.63 Av.: 2.05 f(x,y): 2.260
 Maximum found [x,y,f(x,y)]: [0.62,2.26]

8. Simulation

The simulation is performed on the MATLAB and the various parameters like end 2 end delays and packet delivery ratio are analyzed. The immune algorithm parameter is the objective function. The simulation results in pdr 99% and the end 2 end delay is 1.5 ms. The Objective function is minimized by using the number of iteration and the plot shows the result.

While program is executed then:

**** Clonal Selection Algorithm - CLONALG ****

Number of generations: 25

Population size: 100

Mutation probability: 0.010

Number of clones per candidate: 10

It.: 1 pm: 0.0100 x: 0.34 y: -0.35 Av.: 0.88 f(x,y): 2.004
 It.: 2 pm: 0.0100 x: 0.09 y: -0.37 Av.: 1.02 f(x,y): 2.134
 It.: 3 pm: 0.0100 x: 0.09 y: 0.63 Av.: 1.17 f(x,y): 2.205
 It.: 4 pm: 0.0100 x: 0.09 y: 0.63 Av.: 1.26 f(x,y): 2.208
 It.: 5 pm: 0.0100 x: 0.09 y: 0.63 Av.: 1.35 f(x,y): 2.241
 It.: 6 pm: 0.0100 x: 0.12 y: 0.63 Av.: 1.43 f(x,y): 2.241

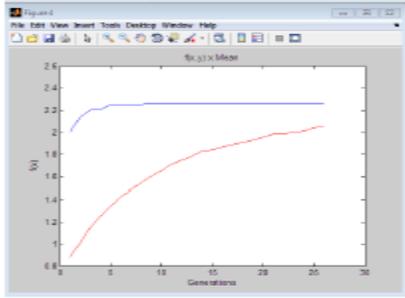


Figure4: Graphical Representation

9. Objective and Future Scope

The packet delivery ratio has been improved to 99% and the network detects the attack quickly and recovery is also done quickly.

10. Future Scope

In future the proposed model can be applied to detect and recover other attacks in the WSN and the model can be used to detect the same attack using different immune algorithm.

References

- [1] I. Akyildiz, W. Su, Y. Sankara Subramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.
- [2] C. Y. Chong and S. Kumar, "Sensor networks: Evolution, opportunities, and challenges," *Proc. IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.
- [3] P. Santi and D.M. Blough. "The critical transmitting range for connectivity in sparse wireless ad hoc networks", *IEEE Transactions on Mobile Computing*, Vol.2, No.1, pp. 25-39, (2003).
- [4] X. Jiang, Y. P. Chen and T. Yu. "Localized distributed sensor deployment via coevolutionary computation", In *Proceedings of 2008 Third International Conference on Communications and Networking in China*, Hangzhou, China, pp.785-789, (2008).

- [5] F. Hu and N. K. Sharma, "Security considerations in ad hoc sensor networks," *Ad Hoc Networks*, vol. 3, no. 1, pp. 69–89, 2005.
- [6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols*, vol. 1, no. 2–3, pp. 293–315, Sep 2003.
- [7] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: a survey," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 52–73, 2009.
- [8] Adrian Perrig, John A. Stankovic, and David Wagner, *Security in wireless sensor networks*, *Commun. ACM*, 47 (2004), pp. 53–57.
- [9] J.R. Douceur. *The Sybil attack*, In *First International Workshop on Peer-to Peer Systems (IPTPS'02)*, Mar. 2002
- [10] 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: CAN Press, 2004, pp.185-191.
- [11] Dasgupta, D, *Artificial Immune Systems and Their Applications*. Berlin: Springer-Verlag, 1999
- [12] Dasgupta, D, Forrest, S, "Artificial immune systems in industrial applications," *IPMM'99. Proceedings of the Second International Conference on Intelligent Processing and Manufacturing of Materials*.1999,1:257-267.