Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

6th International Conference
on Electrical Engineering
ICEENG 2008

Intrusion Detection System Based on Artificial Immune System for Wireless Sensor Network

By

M. A. Shedid * R. Abo Alez ** A. A. El-Hennawy***

Abstract:

Wireless Sensor Network (WSN) is an advanced computer network which depends on mobile communications. It can be applied for data acquisition in hazardous, home and office environments so that securing working environment for WSN is necessary. Due to inherent limitations in wireless sensor network (limited processing power, storages and energy), security for these sensor networks is not easy. Since sensor networks pose unique challenges, traditional security techniques cannot be applied directly. Intrusion Detection System (IDS) is a must for this critical application. Providing adaptive new intrusion detection systems remain a challenging research problem. In this paper we develop an intrusion detection system that is inspired by the Biological Immune System (BIS).

The idea is to map BIS elements for the detection system in WSN. For examples, the human body is mapped to the entire wireless sensor network; Self cells are mapped to well behaving nodes and non-self cells are mapped to misbehaving nodes, etc. In this proposal we present the integration of some useful immunological function to develop a robust and intelligent detection system.

Artificial Immune System (AIS) is applied in this paper toward developing secured wireless sensor networks using intelligent technology. As a result of using AIS to build IDS the WSN become more secure and immune.

---

* Egyptian Armed Forces
** Al Azhar University, Faculty of Engineering, Cairo, Egypt
*** Ain Shams University, Faculty of Engineering, Cairo, Egypt

Keywords:

Wireless Sensor Network, Intrusion Detection System, Biological Immune System, Artificial Immune System.

1. Introduction:

Wireless sensor network (WSN) has received significant media attention in recent years. In 2003, MIT's Technology Review magazine called it "One of the ten technologies that will change the world"[1]. Applications of WSNs are numerous and growing, some of them are even security critical, like military applications. The ideal wireless networked sensor should be scaleable, consumes very little power, smart and software programmable, capable of fast data acquisition, reliable and accurate over the long term, costs little to purchase and install, and requires no real maintenance [2]. A generic wireless sensor network is composed of a large number of sensor nodes scattered in a terrain of interest, called the sensor field. Each of them has the capability of periodically collecting data about an ambient condition and sending data reports to a central node [3, 4,5].

WSN contains a large number of sensing devices which are limited in energy. Each sensor node comprises sensing, processing, transmission, mobilizer, position finding system, and power units. A wireless sensor network is vulnerable to security attacks, so that it needs un-classical security techniques. The human body shows us how a robust infection defense system can be built.

The biological immune system has the job to keep the body healthy. This system is very complex and uses advanced mechanisms for detecting and eliminating infectious pathogens. The immune system learns how to recognize new pathogens which are intruding the body and then produces the right kind of response to fight them [6,7]. It has many properties which can be adopted for the design of artificial immune systems in the wireless sensor networks security field. The immune system uses anomaly detection for the recognition of pathogens. To provide a secure wireless sensor networks, we need to deploy a similar detection system for intrusion.

In this paper, we will present a survey of the challenges in the security domain for the sensor network in Section 2. Overview about intrusion detection is presented in Section 3. Background and brief illustration about the biological and artificial immune system is presented in Section 4. Related works are presented in Section 5. Then introducing our proposal for intrusion detection system for wireless sensor network based on artificial immune systems is presented in Section 6. Finally, we will present the conclusions and future work.

2. Challenges in the security domain in the sensor network:

WSN are deployed in battlefields or used for monitoring in homeland, the messages exchanged through the WSNs become the target of adversaries; these adversaries can pose many security threats [1,3,5]. The mentioned application fields have mandatory security requirements. The hardware and energy constraints of the sensors add difficulty to the security requirements concerning availability, confidentiality, authentication, integrity, and non-repudiation. Availability ensures the survivability of network services despite denial-of-service attacks. Confidentiality ensures that are exchanged message is never disclosed to unauthorized entities. Integrity guarantees that a message being transferred is never corrupted or modified. Authentication is the process of verifying an identity claimed by or for a system entity. Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message [1,3,6].

The major threats related to the security in sensor network are summarized as Eavesdropping, message injection, message replay, message modification, impersonation, denial of service, malicious code, traffic analysis, and side-channel analysis [1,3,9].

Since WSNs may operate in a hostile environment, security is crucial to ensure the integrity and confidentiality of sensitive information. To do so, the network needs to be well protected from intrusion and spoofing. The constrained computation and communication capability of sensor nodes make it unsuitable to use conventional encryption techniques. Lightweight and application-specific architectures are preferred.

3. Intrusion Detection:

Intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified [6]. An intrusion can be defined as "an act of a person of deputy attempting to break into or misuse a system in violation of an established policy".

The main goal of any intrusion detection system IDS is to detect any intruder who tries to infringe or access the system. The objective of the intruder is to gain access to a system or to increase the range of privileges accessible on a system. Intrusion detection is an important part of wireless sensor networks security. It provides an additional layer of defense against network misuse after physical, authentication and access control. Intrusion detection has focused on two major categories: (a) anomaly based intrusion detection, (b) misuse intrusion detection [10]. Anomaly based intrusion detection is based on the detection of deviations of the system behavior which is defined by a profile for normal behavior. This profile is learned by the IDS during a long time observation of the network. Thus, the object of anomaly based detection is to detect intrusion based on unusual system behavior. Typically this is done by first developing a profile of the

system in normal use. Once the profile has been generated it can be used to evaluate the system in the face of intruders. In systems based on misuse intrusion detection, the system maintains a database of intrusion signatures. Using these signatures, the system can easily detect intrusions on the network. The information is analyzed by comparing it with pre-defined patterns in a database. IDS that uses misuse detection protects the system as soon as installed with a very low false positive rate. If the IDS signals an alarm it is directly referred to a specific kind of network activity. But those systems do not detect new types of attacks which are not included in the database [9,10]. Intrusion detection is an important issue in security domain in wireless sensor networks.
Intrusion detection is an important issue in security domain in wireless sensor networks. Despite the importance of effective intrusion detection schemes for wireless sensor networks, a good solution has not yet been devised; this is due to the resource constraints existed in wireless sensor networks. Besides, techniques used in securing traditional networks cannot be applied directly to WSNs, since they need resources not available in sensor networks. WSNs are application oriented, which means they are designed to have very specific characteristics according to the target application [5,11]. In fact, wireless sensor networks are vulnerable to many forms of intrusion. In traditional networks, traffic and computation are typically monitored and analyzed for anomalies at various awareness points. This is often expensive in terms of network's memory and energy consumption, as well as its inherently limited bandwidth. Wireless sensor networks require a solution that is fully distributed and inexpensive in terms of communication, energy, and memory requirements.

4. Biological and Artificial Immune System:

In medical science, historically, the term immunity refers to the condition in which an organism can resist disease, more specifically an infectious disease. The biological immune system is an adaptive learning system that is highly distributive in nature. It employs multi-level defense mechanisms to make rapid, highly specific and often very protective responses against a wide variety of pathogenic microorganisms. The biological immune system is a complex adaptive system that exists in vertebrates to protect them from invading pathogens. To accomplish its tasks, the immune system produce a sophisticated pattern of recognition and response mechanisms following various different pathways, i.e. depending on the type of enemy, the way it enters the body and the damage it causes, the immune system uses various response mechanisms either to destroy the invader or to neutralize its effects [8, 12].
The immune system has the great potentiality of being able to build up repertoires of cells and molecules to combat invading disease-causing elements, known as pathogens (e.g., viruses, bacteria and funguses). By modifying the molecular structure of immune receptors and increasing the concentration of particular cells and molecules in the blood

and lymph, the immune system can also become increasingly better at recognizing and destroying these pathogens [7].

There are two inter-related immune systems, the innate immune system and the adaptive immune system, by which the body can detect foreign attacks. The innate immune system is so called because the body is born with the ability to recognize certain microbes and immediately destroy them. Our innate immune system can destroy many pathogens on first encounter. The innate immunity is capable of distinguishing between (self) and (non-self) [7,12,13].

The adaptive immune system uses somatically generated antigen receptors which are clonally distributed on the two types of lymphocytes: B cells and T cells. These antigen receptors are generated by random processes and, as a consequence, the general design of the adaptive immune response is based upon the clonally selection of lymphocytes expressing receptors with particular specificities. The antibody molecules play a leading role in the adaptive immune system. The receptors used in the adaptive immune response are formed by piecing together gene segments. Each cell uses the available pieces differently to make a unique receptor, enabling the cells to collectively recognize the infectious organisms confronted during a lifetime. The biological immune system can be envisioned as a multilayer protection system, where each layer provides different types of defense mechanisms for detection, recognition and responses [6].

Artificial Immune Systems (AIS) are adaptive systems inspired by theoretical immunology and observed immune functions, principles and models, which are applied to complex problem domains. Artificial Immune Systems (AIS) emerged in the 1990s as a new branch in Computational Intelligence (CI).

Table 1 illustrates the relation between Biological Immune Systems and Artificial Immune Systems [6, 7,14].In the framework of IDS Danger Theory [16] there is a link between AIS and IDS, suggests that the immune system reacts to threats based on the correlation of danger signals and linking the immune response directly to the attacker. Artificial Immune Systems develop a set of "detectors" based on a training set, these detectors can all be created before the system is deployed, or/and they can be used for continuous "online" learning. They are also used to distinguish between (self) and (non-self) patterns, or "dangerous" and "non dangerous" patterns [7].

To solve a particular problem from a specific domain, using AIS, one should describe immune components; describe the intersection between these components according to the type of problem that is being solved. Then, identify the elements involved in the problem and how they can be modeled as entities in the particular immune model [8]. Figure 1 depicts the general framework for AIS.

The artificial immune system has two main algorithms. They are negative selection and clonal selection algorithm [7,8,14].

1) Negative Selection Algorithm

The negative selection algorithm is inspired by the maturation of T-cells in the thymus

gland. It is called with such a name because it is based mainly on the biological negative selection principle.The algorithm consists of two stages: censoring and monitoring. The censoring phase caters for the generation of change-detectors. Subsequently, the system being protected is monitored for changes using the detectors generated in the censoring stage. However, this algorithm is reported to be very time consuming. This algorithm detects and eliminates harmful antibodies found in the system. The system generates detectors at random, and if they fail to match all examples from a set of self examples, they are retained. The negative selection algorithm is split into two parts, Censoring part and Monitoring part this illustrated in the figures 2(a) and 2(b).

Table (1): Comparison between the biological immune system and the artificial immune system.

Biological Immune System	**Artificial Immune System**
B-cell, T-cell, antibody	Detector represented as a bitstring
Memory cell	Memory detector
Antigen	Problem to be solved
Antibody	Best solution vector
Antigenic detection/response	Recognition/response to a nonself bitstring
Recognition of antigen	Identification of the problem
Production of antibody from memory cells	Recalling a past successful solution
Lymphocyte differentiation	Maintenance of good solutions (memory)
T-cell suppression	Elimination of surplus candidate solutions
Proliferation of antibody	Use of genetic operators to create new antibodies

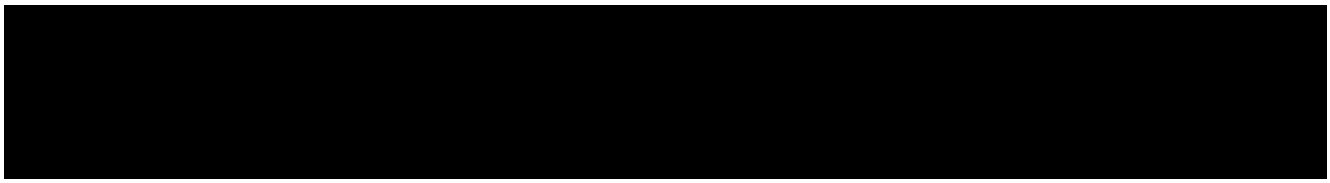

Figure (1): *The general framework for AIS*

2) Clonal Selection Algorithm

The clonal selection is the algorithm used by the immune system to describe the basic features of an immune response to an antigenic stimulus. It establishes the idea that only those cells that recognize the antigens proliferate, thus being selected against those which do not. Clonal selection operates on both T cells and B cells. The main features of the clonal selection theory:

- The new cells are copies of their parents (clone) subjected to a mutation mechanism

with high rates (somatic hyper mutation);

- Generation of new random genetic changes, subsequently expressed as diverse antibody patterns by a form of accelerated somatic mutation;
- Proliferation and differentiation on contact of mature cells with antigens; and the persistence of forbidden clones, resistant to early elimination by self-antigens, as the basis of autoimmune diseases.

The colonal selection algorithm runs as follow:

(1) Generate a set (P) of candidate solutions, composed of the subset of memory cells (M) added to the remaining (Pr) population (P = Pr + M);

(2) Determine (Select) the n best individuals of the population (Pn), based on an affinity measure;

(3) Reproduce (Clone) these n best individuals of the population, giving rise to a temporary population of clones (C). The clone size is aincreasing function of their affinity;

(4) Submit the population of clones to a hypermutation scheme, where the hypermutation is proportional to their affinity. A maturated antibody population is generated (C*);

(5) Re-select the improved individuals from C* to compose the memory set M. Some members of P can be replaced by other improved members of C*;

(6) Replace d antibodies by novel ones (diversity introduction). The lower affinity cells have higher probabilities of being replaced.

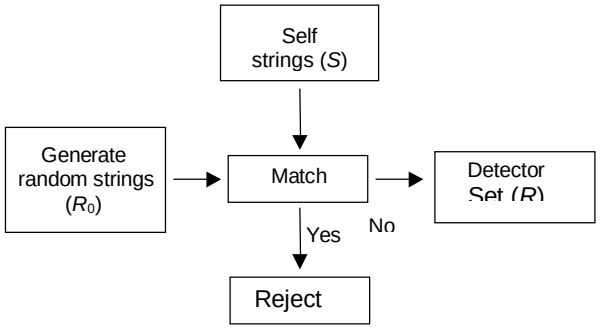

Figure 2(a): Censoring part

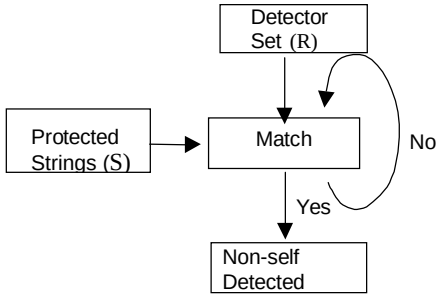

Figure 2(b): monitoring part

5. Related works:

There is relatively little work in the area of intrusion detection techniques for wireless sensor networks. Instead, mainly intrusion detection for specific kind of attacks, like wormhole attacks, routing holes, etc.

One approach works on self-organized criticality (SOC) and Hidden Markov models to

detect data inconsistencies [17]. Developing this approach was based on the structure of naturally occurring events. Hidden Markov models are applied with the acquired knowledge distilled from the self-organized criticality aspect of the deployment region, it. This model allows sensor networks to adapt to the norm of the dynamics in its natural surrounding so that any unusual activities can be identified.

Reference [18] discussed the formula of the attack-defense problem by game theory and used Markov Decision Process to single out the most vulnerable sensor nodes.

In [19], there is a description of a distributed algorithm, BOUNDHOLE, to build routes around the routing holes, which are connected regions of the network with boundaries consisting of all the stuck nodes.

Moreover, there are some papers applying fault-tolerant technologies in providing network security. In [20], secure multi-path routing to multiple destination base stations is designed to provide intrusion tolerance against isolation of a base station. Also, anti-traffic analysis strategies are proposed to help disguise the location of the base station from eavesdroppers. Reference [21] targets the identification of faulty sensors and detection of the reach of events in sensor networks with faulty sensors. It proposed two algorithms for faulty sensor identification and fault-tolerant event boundary detection. These algorithms are localized and scalable for WSNs.

There are many attempts that were applied in Artificial Immune System for Intrusion Detection in traditional network not in WSN, such as LISYS (Lightweight Intrusion detection SYStem) [22,23]. In LISYS, network traffic is monitored. The elements are represented and modeled by binary strings containing the header information of the TCP network traffic.

6. Proposed Intrusion Detection System:

In our proposal we will investigate new method for intrusion detection in wireless sensor network based on artificial immune systems. The intrusion detection depends on detecting the intrusions in the wireless sensor network by sensing uncertain phenomenon from the inspection data. The main problem of detecting intrusion in WSN is to differentiate between (self) and (non-self), (self) is defined as all elements of the network that do not damage the system, (non-self) are all the other elements. The (non-self) set includes all elements that have a negative effect on the continuous functioning of the sensor network.

Detecting a certain intruder for the first time can be viewed as deviation from (self) not by looking from specific intruder pattern.

The normal behavior of the sensor network can be monitored over time. The problem of detecting intrusions can be viewed as finding non permitted deviations of the characteristic properties in the monitored sensor network. If (non-self) elements are

detecting, some action can be taken to eliminate them. In our proposal, sensor network can be assumed as consisting of three levels as shown in Figure 3.

The lower level is the sensors nodes, in which collecting application data and monitoring behavior of neighboring nodes are done. Due to inherent limitations in sensor nodes (limited processing power, storages and energy), we suggest to use low complexity intrusion detection system in this level, depends on negative selection algorithm in which detecting intrusion can be viewed as deviation from (self) not by looking from specific intruder pattern. When it detects intrusion according to (self) and (non self) behavior; the set of data (intrusion patterns) collected by a group of sensor nodes is sent to the related sink node and discriminated. Then this sink node sends this data to the higher level (base station), in which this data is classified and updated at the (non-self) profile.

Then the (non-self) profile is sent to the sink nodes after the updating, then to the nodes once again. Here we can see that any other attempt - might be done by that certain intruder - would be detected faster compared with the first time. And the previous procedure can be called "Learning".

The second level represents the sink nodes which connect sensor nodes distributed in a certain region. A sink node combines the application data from neighboring nodes, monitors behavior of the network or individual nodes, when it detects intrusion by comparing the collected data with the network behavior self and non-self, it isolates the relevant nodes. Each group of sensor nodes connected to the same sink node forms what is called an "area". Then each area is monitored by the proposed IDS. This IDS analyzes and sends results to the next level.

The higher level is the base station, in which we combine both the negative selection algorithm and the clonal selection algorithm. It is a powerful machine, which monitors behavior of the network or individual nodes, updates and sends the (non-self) profile to the lower levels compares the normal behavior with the data from sink nodes then isolates the relevant sink node or relevant nodes. At this level the IDS only analyzes the reports sent from the lower level. The assumed architecture gives us better scalability because the analysis of the data distributed among the different areas of the network. Our proposal consists of three phases which are learning phase, classifying phase and detection phase. In the learning phase, our application tries to build the dataset that will be used in the detection and classification phases. The learning dataset is created through running the application in a safe environment (supervised learning technique) to create the antibodies that will bind to the antigens (packets) of the new cells (sensor network nodes).Table 2 defines terms used in our proposal.

The influential variables in our proposal and some of their effects are Genes, Antigenes, Number of antibodies in a detector, contents of self and nonself, Length of self and nonself, Affinity threshold, and Antibody length.

Figure (3): *Sensor Network in Our proposal*

Table (2): *Definitions of terms used in our proposal*

Term	Definitions
CDS	Collected Dataset
CDSTimer	The maximum time for learning phase
DS	Dataset list
NOCDS	Number of elements in the Collected Dataset
Antigene	The behavior of the each node, it consists of genes from which the node can be classified as self or nonself.
Antibody	a pattern with the same format as the compact representation of antigen
DetectedMisbNodes	A list containing the nodes detected as misbehaving
MisbProbability	A list containing the nodes probabilities of occurrence to be misbehavior nodes
currentProb	A variable that contains the current probability to be checked
threshold	According to this value, we determine if this node is classified as misbehavior node or not
ClassifiedMisbNodes	A list that contains the nodes classified as misbehavior nodes

Learning Phase:

The algorithm starts with an initialization phase through which we free the detector scores (to release any garbage resident in memory), then we set a flag that will enable us to continue looping and collecting antigens (packets) through which we will build our initial antibodies that will be updated through the application running, we also reset a variable i that will help us to iterate through the list of detector set.

The algorithm starts its work by a stimulus (Packet Sent Received Or

Overheard) in a certain interval of time for which the node sends the packet is monitored, then we start to collect antigens (Self-antigens) for each node from the preserved genes, which our algorithm only consider, the algorithm works in protected environment, our algorithm starts to update the nodes' neighbors list (NL), with the new packet and the new data. After that, the algorithm tests whether the number of collected datasets (NOCDS) equals the maximum number of collected dataset (Max Num Of CDS) at which the algorithm can stop and begins to create its initial detectors using the negative selection process. The algorithm uses the antigens collected at this training phase and creates patterns which are not like the antigens collected in this phase. Then it starts its journey to detect, classify and learn with new types of attacks. A flow diagram of the learning phase is presented in Figure 4.

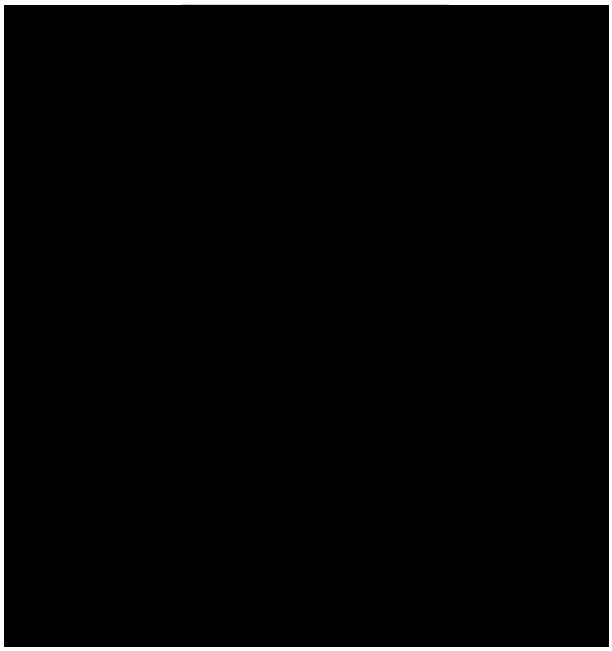

Figure (4): *A flow diagram of the learning phase*

```
  CDS = 0;
  CDSTimer =Estimated learning time;
  DS[0]= CreateEmptySetOfDetectors();
  i = 0;
Flag = true;
While (Flag)
      //Begin while
       If (PacketSentReceivedOrOverheared)
```

```
//Begin if
        NL = UpdateNodesList();
        If (NOCDS < MaxNumOfCDS)
            CDSTimer = CDSTimer- timeElapsed;
            i++
            DS[i] = CreateNewDataSetOfDetectors();
        endif
    endif // stimulus
endWhile
```

Classifying and Detection Phase:

In the Classifying and Detection phase, the algorithm starts its work as in the training phase, until the collected data reaches the rate at which it can be applied to bound to the antibodies created during the learning phase, then the affinity measure with the collected antibodies, which will tell whether it is a misbehavior or not. Then the algorithm starts to update its dataset by cloning such patterns that has an affinity measure of a misbehavior node. The cloning process continues to work until it finds an antibody specific probability to the misbehaving node at which the algorithm preserve this antibody to represent a secondary response from which the algorithm will detect such misbehavior in the future cases to recognize such misbehaves.

Additionally, the algorithm will finish the lifetime of antibodies that do not bind to any antigens. A flow diagram of the classification and detection is presented in Figure 5.

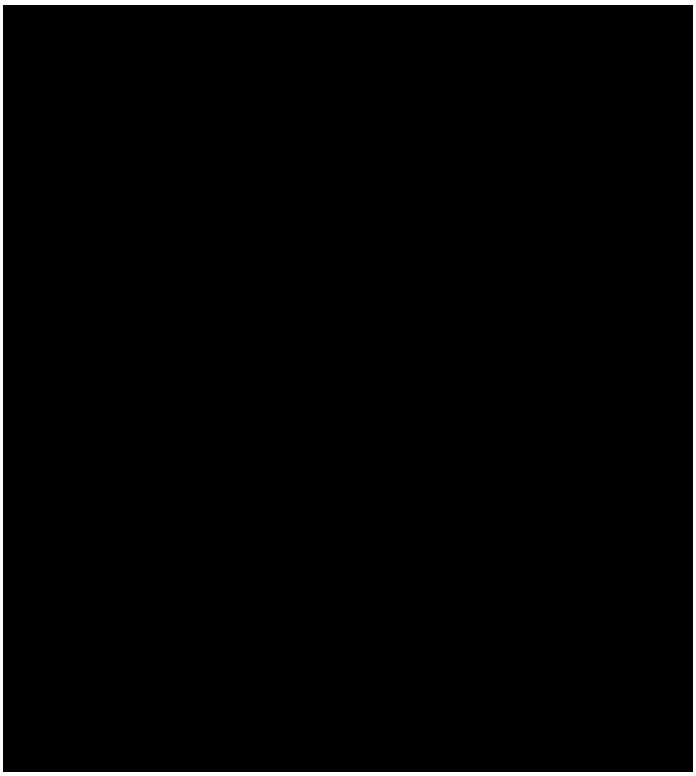

Figure (5): *A flow diagram of the classification and detection*

```
Antigenes = CreateAntigenesList( );
Antibodies = GetAntibodiesList( );
While Not end of list (Antibodies)
        Antibody = GetNext(Antibodies);
        While Not end of list (Antigenes)
                Antigene = GetNext(Antigene);
                If(!Affinity(Antibody , Antigene))
                        Update(DetectedMisbNodes);
                        Update(MisbProbability);
                End if
        End while
End while
While Not end of list (MisbProbability)
        currentProb = GetCurrent(MisbProbability)
        if currentProb > threshold
                AddNodeTo(ClassifiedMisbNodes)
        End if
End while
```

7. Conclusions:

We conclude that there is a link between AIS and IDS, suggests that the immune system reacts to threats based on the correlation of various signals. AIS links the immune response directly to the attacker.

The central challenge with WSN security is determining the difference between normal and potentially harmful activity. The biological Immune System (BIS) can detect and defend against harmful and previously unseen invaders, similar to Intrusion Detection System (IDS) against intruder. The main goal for our proposal is to detect and identify the non-self patterns within a potentially larger set of existing self patterns.

In this proposal we present the integration of some useful immunological function to develop a robust and intelligent detection system. This proposal will enable the user of better monitoring to the sensor network and give an additional feature to the sensor network to become secured and immune. The intrusion detection systems proposal is more flexible and intelligent enough to detect both known and unknown intrusions.

Artificial Immune System was applied in this paper toward developing secured

wireless sensor networks using intelligent technology. We should be able to make wireless sensor networks much more secure than they currently are.
As wireless sensor networks continue to grow and become more common, we expect that further works of security will require these wireless sensor network applications. We 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.

References:

[1] A. Hac, "Wireless Sensor Network Designs", John Wiley& Sons, Ltd, 2003.

[2] Jon S.Wilson, "Sensor Technology Handbook" Elsevier Inc. 2005.

[3] Nirupama Bulusu Sanjay Jha, "Wireless Sensor Networks ", Artech House, Inc, 2005.

[4] Chee-Yee Chong, "Sensor Networks: Evolution, Opportunities, and Challenges" In Proceedings of the IEEE, Vol. 39, No. 8, August 2003, pp. 1247-1256.

[5] John Zachary," A decentralized approaches to secure management of nodes in distributed sensor networks" Milcom, 2003.

[6] W. Stallings, "Cryptography and Network Security Principles and Practices", Fourth Edition, Prentice Hall, 2005.

[7] Leandro Nunes de Castro, Fernando J. Von Zuben "The Clonal Selection Algorithm with Engineering Applications" Workshop Proceedings of GECCO'00, pp. 36-37, Workshop on Artificial Immune Systems and Their Applications, Las Vegas, USA, July 2000.

[8] Dipankar Dasgupta University f Memphis, USA, "Advances in Artificial Immune System", IEEE Computational Intelligence Magazine, Nov. 2006 pp. 40-49.

[9] A. Perrig, J. Stankovic, and D. Wagner "Security in Wireless Sensor Networks" ACM Vol. 47, No.6, June 2004.

[10] Eric Cole, Ronald Krutz, and James W. Conley , " Network Security Bible" Wiley Publishing, Inc. ,2005.

[11] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," Proc. 10th ACM Conf. Comp. and Commun. Security, Oct 2003, pp. 42-51.

[12] Anil Somayaji, Steven Hofmeyr, & Stephanie Forrest "Principles of a Computer Immune System" New Security Paradigms Workshop Langdale, Cumbria UK,1997.

[13] J. Kim and P. Bentley. "The Human Immune System and Network Intrusion Detection". 7th European Conference on Intelligent Techniques and Soft Computing (EUFIT '99), Aachen, Germany, 1999.

[14] Richard A. Goldsby, T. J. Kindt, B.A. Osborne, Janis Kuby. Immunology, 5th Edition.W. H. Freeman and Company, New York, 2003.

[15] Paul K. Harmer, Paul D. Williams, Gregg H. Gunsch, and Gary B. Lamont, " An Artificial Immune System Architecture for Computer Security Applications", IEEE Transactions on Evolutionary Computation, Vol. 6, No.3, June 2002.

[16] U Aickelin, P Bentley, S Cayzer, J Kim, J McLeod "Danger Theory: The Link between AIS and IDS?"2nd International Conference on Artificial Immune Systems, 2003.

[17] S. s. Doumit, D. P. Agrawal, "Self-organized Critically & Stochastic Learning Based Intrusion Detection System for Wireless Sensor Networks," MIL COM, October 2003

[18] A. Agah, S. K. Das, K. Basu, "Intrusion Detection in Sensor Networks: A Non-copporative Game Approach," IEEE International Symposium on Network Computing and Applications, 2004.

[19] Q. Fang, J. Gao, L. J Guibas "Locating and Bypassing. Routing Holes in Sensor Networks," IEEE INFOCOM'04, March 2004.

[20] J. Deng, R. Han, S. Mishra,"Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks," IEEE International Conference on Dependable Systems and Networks (DSN), 2004, pp.594-603.

[21] M. Ding, D. Chen, K. Xing, and X. Cheng, Localized Fault-Tolerant Event Boundary Detection in Sensor Networks,", IEEE INFO COM, 2005.

[22] J. Balthrop, S. Forrest, and M. Glickman. Revisiting lisys: Parameters and normal behavior. In CEC-2002: Proceedings ofthe Congress on Evolutionary Computing, 2002.

[23] S. Hofmeyr and S. Forrest. Architecture for an Artificial Immune System, Evolutionary Computation, 2000.