November 2018

A Study on the Adaptability of Immune System Principles to Wireless Sensor Network and IoT Security

Vishwa Alaparthy
University of South Florida, vishwateja@mail.usf.edu

A Study on the Adaptability of Immune System Principles to Wireless Sensor Network and IoT Security

by

Vishwa Alaparthy

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy in Electrical Engineering
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Salvatore D. Morgera, Ph.D.
Gangaram Ladde, Ph.D.
Nasir Ghani, Ph.D.
Christopher Passaglia, Ph.D.
Selcuk Kose, Ph.D.

Date of Approval:
November 6, 2018

Keywords: WSN's, IoT's, IDS, Danger Theory, Human Immune System, Negative Selection, RPL

ACKNOWLEDGMENTS

I am truly indebted to my supervisor, Dr. Salvatore Morgera, for his guidance, support and constant encouragement during my Ph.D. study. I owe an incredible amount of gratitude to Dr. Selcuk Kose for his constant motivation and encouragement during the course of my degree. I would like to thank Dr. Christopher Passaglia for his insight, invaluable suggestions and comments. I want to thank Dr. Nasir Ghani, Dr. Gangaram Ladde for serving on my committee; and for their precious time and suggestions. I would also like to acknowledge Dr. Christos Ferekides and the staff from the Department of Electrical Engineering at USF, who have always been very helpful, supportive and kind.

I am particularly grateful to my dear friend; Amar Amouri for his encouragement, support, collaboration and enlightening discussions.

Words are not enough to express deepest gratitude to my parents, grand- parent and my sister; for their relentless support, encouragement and supplications throughout my life.

I would not find enough courage to finish Ph.D. without the moral support of my friends, therefore I would like to express my special thanks to them: Siddhartha Nalluri, Varun Korukonda and Sadhu Moka.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Network security has always been an area of priority and extensive research. Recent years have seen a considerable growth in experimentation with biologically inspired techniques. This is a consequence of our increased understanding of living systems and the application of that understanding to machines and software. The mounting complexity of telecommunications networks and the need for increasing levels of security have been the driving factor. The human body can act as a great role model for its unique abilities in protecting itself from external, foreign entities. Many abnormalities in the human body are similar to that of the attacks in wireless sensor networks (WSN). This paper presents basic ideas drawn from human immune system analogies that can help modelling a system to counter the attacks on a WSN by monitoring parameters such as energy, frequency of data transfer, data sent and received. This is implemented by exploiting two immune concepts, namely danger theory and negative selection. Danger theory aggregates the anomalies based on the weights of the anomalous parameters. The objective is to design a cooperative intrusion detection system (IDS) based on danger theory. Negative selection differentiates between normal and anomalous strings and counters the impact of malicious nodes faster than danger theory. We also explore other human immune system concepts and their adaptability to Wireless Sensor Network Security.

CHAPTER 1: INTRODUCTION

1.1 Motivation and Background

The Wireless Sensor Networks (WSN's) are a network of low-cost, low-energy devices that are designed and programmed to work in harsh environments with little or no infrastructure [1]. Devices, or nodes, are densely distributed across areas ranging from those associated with a local area network to a network spanning different continents. These devices or nodes are provided with an ability to sense, store, transmit and receive data over various channels. To achieve these provisions, these devices are equipped with different modules such as a microcontroller, storage unit, transceiver, antenna, and power supply [2]. These networks are largely deployed in military, environmental and health monitoring. These sensor nodes are generally deployed over extended periods, sensing and transmitting data to a server. The nodes communicate and transmit the data among themselves enroute to a sink node. The sink node collects the data from its subsidiary nodes and has the capabilities to perform calculations, if required; aggregate data; and act as a gateway to the Internet. These networks can either be homogenous or heterogenous depending on the sensed data [3]. Although most sensor networks are homogenous, heterogenous networks are not uncommon. These nodes need not have a definite position. They can be deployed in a random manner and the topology does neither have to be pre-defined, nor constant in time. Such networks require a self-organizing capability among the nodes as the network changes its topology.

Wireless Sensor Networks have seen an explosive growth both in their volume of usage and research conducted over the past few years, and this rate is anticipated to accelerate at a considerable pace. This, coupled with their necessity in mission critical applications, makes data security a significant area of concern. Due to their limited resources [4] and the harsh environments in which they are sometimes deployed, it is a challenging task to secure them from attack. Hence, a parallel trail of research is being performed on securing these networks. Apart from the conventional techniques employed to secure a network, there has been an emergence of an alternate field of security mechanisms using bio- or immune-inspirations as a source.

Successful behavioral and communication stratagems of a biological network can serve as an inspiration to model and manage a wireless network. This can be due to the fact that the sophistication provided by a biological network is very intriguing and intuitive. Also, the robustness provided by a biological network is noteworthy and truly unique. This coupled with the need for lower power dissipation and suboptimal energies in a wireless sensor network make the human body a great source of inspiration. The large volume of research in bio-inspired Intrusion Detection Systems (IDS) is also due to the inadequacy of successful conventional techniques. Providing security to a wireless network has always been a difficult task. Although various levels of security have been provided to a system or a node, adversaries tend to find a way to break through these layers. The affected node can divulge some information or sometimes turn into an attacker. The operational strategies of a WSN, and, in particular, the multihop approach to data movement from source to sink, also considerably weakens the security measures of the system [5]. Due to such numerous challenging aspects of designing a security system, a self-adaptive, self-healing model is essential. Due to the complex nature of human body and its ability to protect itself from external pathogens, it is considered a perfect role-model. Many successful techniques have been put forward over the years related to the security of wireless networks.

Security to be provided to WSNs falls into different levels. While the first level deals with evading intrusions, the second deals with detecting an intrusion. The third level provides an intrusion response which can be of varied approaches. Cryptography and firewalls are the most preferred forms of securing a WSN from an attack. Intrusion detection is obligatory when an adversary manages to penetrate the firewall and causes complications with the privacy, confidentiality, and authenticity of the information in the network.

1.2 Contributions

This work attempts to build an analogy between the human immune system (HIS) and intrusion detection system (IDS) methods for wireless sensor networks. This is achieved by studying the various immune theories proposed for the HIS and determining which of these appear to be applicable to WSNs. We review three distinct features or theories of the HIS that help to protect itself from external pathogens, namely danger theory, negative selection, and clonal selection and assess their adaptability to WSN IDS design. The subsequent section of this work tries to replicate segments of the HIS in a WSN and then later, attempts to derive an IDS scheme. This is done using the properties of danger theory and negative selection.

As mentioned earlier, WSN's pose some restrictions in terms of memory and energy consumption. This dissertation proposes a multi-level IDS based on danger theory, which cannot only detect an attack but can also adapt to those attacks, while taking all the mentioned factors into consideration. While most IDS's are confined to detecting a single attack, this model can detect a wide variety of attacks. This is made possible by operating with a variable called the *aggregator output*. Another important feature of this algorithm is that it can detect and adapt to unknown attacks. Although there have been attempts to use danger theory for WSN design in the past, they lack features such as adaptability, detecting a variety of attacks, which the current model possesses. It should also be mentioned that to our knowledge danger theory has never been used as a model for IDS design in networks using low power routing protocols such as RPL. The model presented here, however, supports the RPL protocol and low power protocols similar to it. While working with danger theory, the WSN is treated as a HIS and parallels are drawn between the nodes and the immune cells, and certain tasks are assigned to the nodes. Danger theory is applied as an adaptive immune response which is a combination of anomaly-based and signature-based techniques. None of the IDS designs in the literature based on danger theory had combined both anomaly-based and signature-based techniques. The concentrations of some features, such as energy dissipated, number of packets sent and received, frequency of data transfer are matched with their respective weights and a variable called the aggregator output is generated.

In the sequel, negative selection is used is lieu of danger theory to model an IDS for WSN's and the results are presented. Negative selection is generally not preferred in designing IDS's for WSN's, especially for RPL protocol, due to the number of detectors it generates. However, this work uses features such as time duration, time interval between transfers, data sent and received, number of hops, type of connection, etc. to create a minimal length string which is used to determine self- and non-self-patterns. The whole length of the string need not be used during the detection process. This makes the model more effective in different situations. Non-self-strings are stored for detection while discarding the self-patterns or strings. This process is done by measuring the Euclidean distance between the strings. These non-self-patterns are later used to detect the malicious patterns in the network using an immune matching technique called r-bit contiguous matching. By using this technique, this model was able to detect the attacks using the least number of features, thereby saving memory and energy. In conclusion, this model developed in this work optimizes the use of features and energy to permit a more efficient use of the negative selection algorithm than other contemporary IDS designs found in the literature. Advantages and limitations of both IDS models are also studied and presented.

In addition to this, the nodes in a WSN are tested with a novel set of attacks called schizophrenic attacks which are modelled on a node which switches its state between normal and malicious using uniform distribution. These attacks are not mentioned in the literature and are designed exclusively for this dissertation. The performance of the HIS inspired algorithm on these schizophrenic nodes is tested and the results are presented and compared to other IDS's.

In summary, the contributions of this dissertation are:

1) Investigation of different immune theories such as danger theory, negative selection, clonal selection etc. and assessment of their applicability to WSN security.
2) Model an IDS based on danger theory. Some unique contributions and features of this model, which differentiates it from other IDS's include

- Can detect and learn known as well as unknown attacks.
- Can detect a wide variety of attacks.
- Multi-Level, with both anomaly and signature-based techniques.
- Ideal for low power routing protocols.
- Conserves memory and energy.

3) A comparison of the proposed danger theory-based IDS with some of the contemporary detection techniques for WSN's.
4) Model an IDS based on Negative Selection. Some unique contributions and features of this model, which differentiates it from other IDS's are

- Minimal string lengths, memory and energy.
- Ability to choose the number of features to be used.
- Faster detection times.

5) Formulation of new attacks called schizophrenic attacks and use of the new IDS models and conventional IDS designs to test network integrity under these attacks and draw comparisons.

1.3 Dissertation Roadmap

The remainder of this work is organized as follows.

Chapter 2 provides a brief literature survey on the work done on Intrusion Detection Systems based on Bio and Immune inspired techniques.

Chapter 3 gives information about the security specifications and the vulnerabilities in a WSN along with a section describing the WSN's layers of defense which includes a basic classification of the IDS's in WSN's.

Chapter 4 provides a brief overview of the Human Immune System (HIS) and the theories put forward, which aid the functioning of the Immune System. It also gives an idea of how to create an Artificial Immune system (AIS) for a WSN based on the afore mentioned theories.

Chapter 5 describes the manner in which an analogy is derived and puts forward the functional mechanism of the IDS, which is inspired from immune techniques such as danger theory and negative selection.

Chapter 6 presents the modelling of the attacks, parameters used, simulations and discussions on the results obtained.

Finally, Chapter 7 concludes this work and presents topics for future research.

CHAPTER 2: LITERATURE SURVEY

2.1 Bio Inspired WSN Security

Several IDS have been designed based on biological models [6.7] and Artificial Immune Systems (AIS) [8] is one such model. Neural networks [9], Swarm intelligence [10] and ant colony optimization algorithms (ACA) [11] are some of the most common biologically inspired algorithms for network security apart from immune theories. While neural networks derive an inspiration form the human nervous system, Ant clustering algorithm is inspired by the movements of a number of artificial ants which is used to form clusters. This algorithm makes use of the behavior of the ants when they are subjected to threats. More specifically, the nature of the ants to form a cluster as a defense mechanism and go back to their normal states when the threat is subdued is adapted to wireless sensor networks.

Hao et al. proposed a defense mechanism called AraTRM, which makes use of Ant Colony Optimization [12]. It assigns scores to each node in the transmission path from the destination to source as the data is passed through it and identifies the malicious node.

Kulkarni et al derived an intrusion detection system which has low storage and low computational times based on neural networks [13]. This scheme detects denial of service (DOS) attacks based on collision rates and the arrival rates of the data packets. Although this scheme uses minimal energy, it tends to produce a sizeable number of false positives.

Bitam et al [14] proposed a security mechanism based on swarm intelligence, which allows the network to adapt to the attacks. This model has a light weight approach designed and enables efficient task monitoring and allocation of the resources along with detecting a wide variety of attacks such as Sybil or DoS.

Fulp et al [15] proposed a genetic algorithm based on the configurations of the system. The configurations are simplified as chromosomes and a fitness level is accorded to the system. The existing configurations or chromosomes are used to derive a new set of chromosomes. The system security is proportional to the fitness of new configurations, enabling it to detect a variety of attacks.

2.2 Immune Inspired WSN Security

As mentioned earlier, AIS is inspired by human immune system and has capability to differentiate normal and abnormal states. HIS-based IDS designs are mostly centered around two theories, Negative Selection (NSA) [16] and Danger Theory [17]. While Negative Selection deals with identifying self and non-self-entities, Danger Theory revolves around danger signals which are emitted by the Dendritic cells when an intrusion or an anomaly is detected. Clonal Selection [18] is also used to devise an Artificial immune system; however, Clonal Selection is primarily used in conjunction with Negative Selection. Positive Selection [19] is another theory which also identifies the self and non-self entities; however, the censoring is done from a randomly generated data set by eliminating the non-self entities as opposed to negative selection, which bases itself on recognizing the self entities and editing them out. The remainder of the data set is stored as a detector set. NSA is bound to produce a large number of detector sets and is generally not suitable for dense environments. Danger Theory does not necessarily generate a large dataset and has fewer false positives than the NSA and Clonal Selection. More details of these techniques and its adaptability to wireless sensor networks is studied in the later parts of this work.

Hosseinpour, et.al. [20] introduced a detection mechanism based on innate immune properties using an unsupervised machine learning approach. In this work, an AIS is designed to detect and adapt to unknown attacks and zero-day attacks. This algorithm is based on identifying self and non-self-patterns, which is the core of negative selection. Their algorithm has a false positive rate of 0.008 and a true negative rate of 0.991 with an accuracy of 0.771. The authors also showed a recall rate of 0.589 and an anomaly precision of 0.987.

Greensmith et al. used danger theory to build an artificial immune system to help detect intrusions in computer networks [21]. This algorithm produced a set of safe and danger signals based on the phases of dendritic cells. The state of the entire system is switched from safe to danger and from danger to safe when the attack passes. The accuracy of detection is claimed to be 0.99.

Kim et al used negative selection along with a clonal selection operator. The normal activities of the system are classified as self and the abnormal activities are classified non-self [22]. The network protocols such as TCP, UDP and TCMP are clustered after assigning a gene value and a set of detector genotypes are derived and are matched to the normal genes which are derived from the network profile. A fitness level is determined based on the match count. The authors showed a true positive rate of 96.52, 95.55 and a false positive rate of 10 and 7.13 for different datasets.

Forrest et al is one of the early attempts at an AIS to computer networks. It uses negative selection algorithm to discriminate between self and non-self of the network [23]. However, the authors encountered problems with the computational ability of the system. The authors showed a failure probability of 0.27. The detection probabilities were 0.38 and 0.76 for 50 and 100 detectors respectively. This algorithm used a contiguous matching technique to match the antigens and the detectors.

Vidal et al derived an AIS to counter DoS attacks. This algorithm can detect and adapt to unknown attacks [24]. Their algorithm has true positive rates of 98.66, 100 and 99.03 and a false positive rate of 1.42 for different entropies. The authors also backed their algorithm with a mitigation technique for DoS attacks. While their first stage of detection has an accuracy of 81.4%, the second stage was able to detect a DoS attack with a 95.4% accuracy.

CHAPTER 3: SECURITY IN WIRELESS SENSOR NETWORKS

3.1 Security Specifications of WSN’s

The basic specifications for any Wireless Network, including a WSN, adhere to some general requirements. Owing to the unique nature of WSN’s, additional security features such as data freshness, localization, and self-organization are required. The complete set of requirements for a WSN may be found in [25], [26], [27], [28], [29], [30] and is discussed below.

1) Data Confidentiality: Both the sensed data and the routing information is critical to a WSN. Ensuring that the adversaries or any other unauthorized users do not gain access to the network is extremely crucial, especially for mission critical applications such as military surveillance. This is usually achieved by encrypting the data by using a set of keys.

2) Data Integrity: The high node density in a wireless sensor network has every chance to make the system redundant and thereby compromise the accuracy and consistency of the data. Compromise in the integrity of data typically occurs due to faulty communication signals or due to an attacker’s intention to masquerade or tamper with the data transmitted. The networks base station or sink generally detects these types of anomalies when the data is aggregated.

[1] Parts of this chapter were published in IEEE Access, 6, pp.47364- 47373,2018. Permission is included in Appendix A.

3) Self-Organization and Secure Localization: Nodes that are closer to each other are friendlier and complement each other through the hierarchy of service. That is, the nodes closer to each other possess more trust towards each other. A localization algorithm is supposed to take these factors into consideration. These nodes must be efficient enough to identify and verify their own position in a network and their range in the network. Due to the distributed nature of Wireless Sensor Networks, a self-organization protocol is put in place. All the nodes in a sensor network are independent of each other and are supposed to be spontaneous and efficient in their organization.

4) Data Authentication: Due to the distributed nature of the Wireless sensor nodes, authentication is required at both the user end and at the sensing node. A Wireless Sensor network expects multiple concurrent and secure data sessions during its lifespan and thereby needs multiple authentication requests and a protocol to enable it.

5) Data Freshness: Nodes in the sensor network tend to cache the data locally and transmit it to its data aggregator. The sensed data in a WSN environment is very frequent and recurring. It is imperative that this data implies the current state of the sensed environment.

6) Data Availability: Availability is the statistical measure of the probability of the network being serviced at a given instant of time. As most Wireless Sensor networks are resource and data demanding at regular intervals of time, it is crucial that the availability factor is at an optimal level.

3.2 Attacks on WSN’s

WSN’s are largely employed in hostile environments with little or no supervision. This factor along with the acute power and memory constraints make them more susceptible to external attacks. These attacks can be either targeted on the hardware associated [30] or the data transmitted on the network [8]. These data centric attacks are further classified into passive and active based on their inclination to interrupt the network [31] Most of the attacks on WSN primarily focus on imposing three effects which subsets of, or are the causes for, several more anomalies in the system including

- data confiscation and alteration
- packets and noise injection
- increase in redundancy and Latency

Below are a range of firmware and software related attacks which are currently effecting WSN’s. Table 3.1 provides an overview of the attacks discussed below, emphasizing the parameters associated with each attack.

1) Sybil [32]: The attacker node attempts to forge its identity to its peers and decoys the other nodes to pass information through it or transmits fake data packets into the network. This is achieved by replacing the MAC address or IP address of a node in the network. These types of attacks are highly critical and are a threat to the data integrity and confidentiality of the network.

2) Eavesdropping [33]: Eavesdropping is a form of passive attack. Passive attacks are linked to the privacy of the networks and does not alter or steal any data. The attacker either tries to grasp the data from the effected node or through the link between the nodes. The adversary tries to monitor the network traffic and control the node and make it malicious.

3) Wormhole [34]: The attacker tends to capture the data packets from one cluster or a specific location and send it to a distant node in a different cluster and then transmit the data locally. Wormhole attacks are a serious threat to the routing and Localization of the networks.

4) Blackhole [35]: Blackhole attack, which is also called as packet drop attack gets the intermediate node to drop the packets before it reaches its destination. The intermediate node may be the attacker or just an affected node. Loss of links or exhausting the nodes resources may also be the cause for a blackhole attack.

5) Spoofing [36]: The situation in which an adversary pretends as a node in the network and starts sending fake route information and error messages. This attack reroutes the data by altering the routing information and creating fake paths to the destination.

6) Flooding [37]: The adversary attempts to send multiple route requests in a loop to a non-existent node and makes sure all the node resources are depleted. This, in turn affects other nodes in the system by attributing them, some serious resource constraints.

7) Selective Forwarding [38]: As the name suggests, the nodes forward the data selectively. The malicious nodes discard some data packets and send some data packets based on either time or nature of the packets.

8) Traffic Analysis [39]: This attack is based on the Eavesdropped information. It decodes the communication patterns of the network and tries to gather the information about the topology of the network. This attack can be achieved using Rate monitoring, Time correlation and ID analysis.

9) Camouflage attack [40]: Camouflage attacks are used for privacy analysis. A malicious, hidden node is inserted in the network which performs network analysis.

10) Misdirection [41]: The attacker switches the packets to a different node rather than the intended node resulting in the increase of latency. If the data does not find an alternative path, it will be ultimately discarded.

11) Jamming [42]: Jamming is achieved by transmitting high power consumption radio signal frequencies like those used in the network, resulting in draining huge amounts of power consumption and also preventing the intended data to reach its destination. That is, the system jams the authentic data through the extensive amounts of malicious data.

12) Collision [43]: When two neighboring nodes disavow the MAC protocol and starts transmitting at the same time and same frequency, packets get corrupted and resources constrained.

13) Path based DOS Attacks [44]: An overwhelming amount of resource usage is the target of a Denial of Service attack. Flooding one or multiple routes of transmission with faulty or redundant packets can prove to be catastrophic for a resource constrained network such as WSN's.

14) Node Replication Attack [45]: Although this attack is similar to the Sybil attack, it can be easily identified compared to the Sybil attack. While Sybil attacks focuses on forge a single node, node replication attack focuses on introducing multiple nodes with similar identities.

15*)* Homing [46]: The adversaries perform traffic analysis for a limited period to decode the location of the nodes and then try to shut the nodes off or physically disable them.

16) Looping [47]: An intermediate node acts as an attacker and helps its neighbor believe that it is the intended recipient of the data and resulting in an infinite loop.

17) Overwhelm [48]: Overwhelm is an attack on the network's sensing component. An overwhelming amount of stimuli is given to the sensors which results in high energy consumption and a degradation of network performance.

18) Hello Floods [49]: The adversary attempts to send multiple HELLO messages in a loop to either a non-existent node or a neighboring node and makes sure all the node resources are depleted. This, in turn affects other nodes in the system by attributing them, some serious resource constraints.

19) Physical Attacks [50]: Since these networks are mostly unguarded and accessible, they are prone to physical damage. The attacks on the firmware of the network such as tampering the nodes and node capture are easily noticed.

3.3 Layers of Defense

The layers of defense in a WSN include Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and Intrusion Mitigation Systems (IMS). While IPS provides the first line of defense by protecting the network from external threats, IDS help to detect the attacks, which cannot be countered by the IPS. IMS has the necessary countermeasures to mitigate and eliminate the threat. Most WSN's cannot afford to have a mitigation mechanism in place owing to its limited memory and capabilities.

3.3.1 Intrusion Prevention Systems

Systems such as firewalls and techniques such as Cryptography are the primary components of an IPS. Design of inexpensive cryptographic techniques has been the crux of most of those solutions. However, these mechanisms should be light weight and minimal energy consuming. Abdelkarim et al gives an illustration of such techniques [51]. These systems should be able to have a low false positive rate since there is possibility of obstructing the normal network traffic. Most of the systems which employ IDS does not necessarily have an IPS since both of them working in tandem can increase the overhead of the resources. IPS generally do not have an IP address associated with it.

Table 3.1 Attacks in Wireless Sensor Networks

Attack	**Type of Attack**	**Parameters Effected**	**Specifics**
Sybil	Active	Latency, Power consumption & Throughput	Replaces MAC or IP address of a node.
Wormhole	Active	Latency, Power consumption	Reroutes the data.
Black hole	Active	Throughput	Drops Packets
Spoofing	Active	Overhead	Masquerades as another node.
Flooding	Active	Power consumption, Throughput	Floods the network with RREQ's.
Eavesdropping	passive	NA	Sniffs the Network.
Selective Forwarding	Active	Throughput	Filters a few packets which are essential to the network.
Traffic Analysis	Passive	NA	Deduces the traffic pattern
Camouflage	Passive	NA	Hidden nodes
Misdirection	Active	Latency	Misdirects the packets to an unintended node.
Jamming	Active	Power consumption	Transmitting radio signals of same frequencies.
Collision	Active	Throughput	Disavow the MAC protocol.
DOS attacks		Bandwidth, Power consumption, Latency	Flooding the bandwidth &other resources.
Homing	Active & Passive	Firmware	Disabling the nodes physically.
Node replication	Active	Latency, Power consumption & Throughput	Replicating multiple nodes
Looping	Active	Latency	Creates an infinite loop.
overwhelm	Active	firmware	Overwhelming amounts of stimulus given to the sensor node.
Hello flood	Active	Power consumption, Throughput	Floods the network with Hello packets.
Physical attacks	NA	Firmware	Causing Physical Damage

3.3.2 Intrusion Detection Systems

A brief classification of intrusion detection systems based on the methods of detection [52] is given in Fig. 3.1. The detection method used in this work is a hybrid of anomaly and signature-based detection methods. Anomaly-based detection involves generating a network profile. These methods include statistical modelling which builds statistical models of the features that the normal network possesses as a reference and comparing them to the actual parameters generated by the network under test [53], [54]. The extent of anomaly is calculated, and an attack is flagged when the anomaly reaches beyond a threshold.

Knowledge-based detection draws a profile based on the previous knowledge of the network under different test cases and uses it to detect intrusions.

The third type of anomaly detection is based on machine learning. This method generally uses the previous states of the network to define the current state and compare it with the actual state of the network. Fuzzy learning, Neural Networks, Bayesian Networks and Markov models are a few examples of machine learning techniques. Supervised learning, unsupervised learning, semi-supervised learning and reinforcement learning are the types of machine learning techniques employed. Signature based detection has a predetermined set of anomalous profiles which will be used to compare with the network under test. This method is known to produce a very limited number of false positives and can detect any known attack which is previously fed to the detector. Specification based intrusion detection is based on a set of rules or specifications developed by a user. These subsets of IDS design are able to identify known and a variety of unknown attacks.

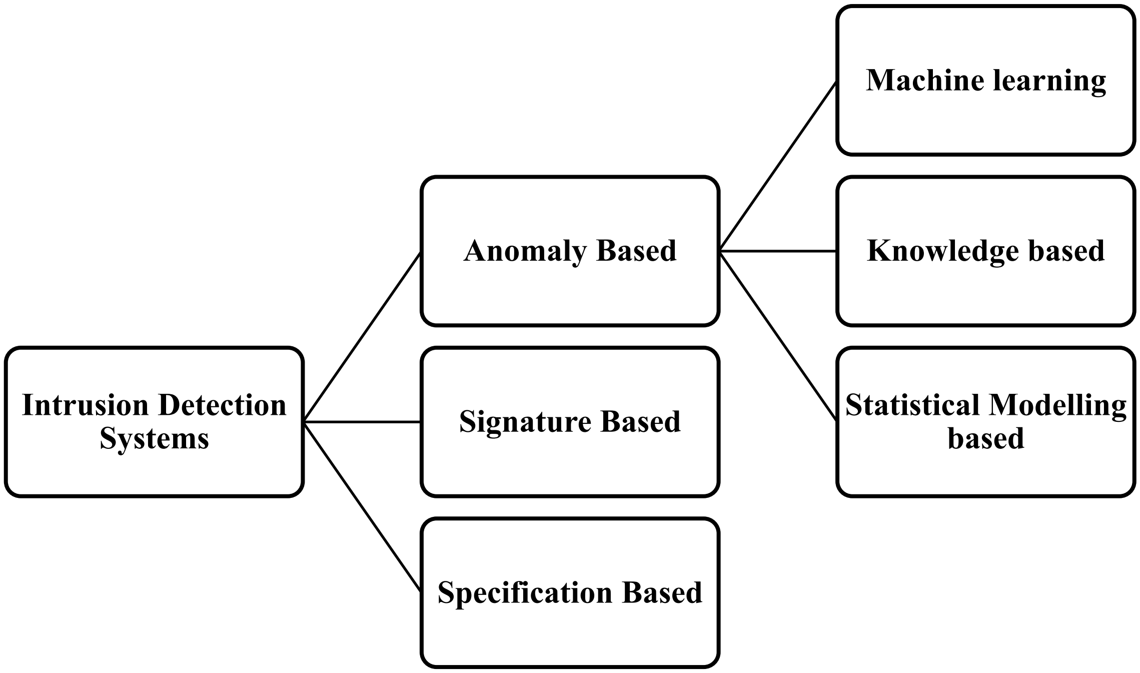


Figure 3.1 Classification of the Intrusion Detection Systems

3.3.3 Intrusion Mitigation Systems

IMS are the third layer of defense. As mentioned earlier, most WSN’s do not have an IMS. Regulating the resources of the malicious node is the most common mitigation technique employed in a WSN. Isolating the node can be done in case of a persistent and high resource consuming attacks. Limiting the rate of resource flow in the network is also an effective technique used. Mishra et al provides a study of intrusion tolerance and mitigation techniques. A fault tolerance mechanism can also be employed to mitigate intrusions [55].

CHAPTER 4: IMMUNE BASED INTRUSION DETECTION SYSTEMS

4.1 Human Immune System

The human Immune System (HIS) is a multi-layered detection, prevention and mitigation structure that provides immunity against a wide range of external pathogens [56]. It is a combination of multiple cells, tissues and organs that are essential for the functioning of the immune system.

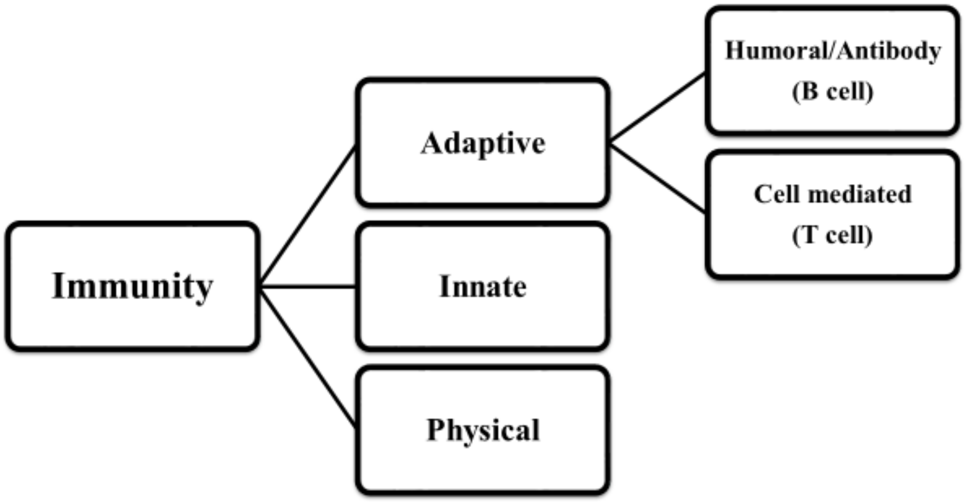


Figure 4.1 Classification of Immune System

[2] Parts of this chapter are to be published in Elsevier Procedia Computer Science, December 2019. Permission in included in Appendix A.

Fig 4.1 describes the types of protective mechanisms from the physical, such as skin, to the adaptive system, which is a subsystem of the overall immune system that is composed of highly specialized, systemic cells and processes that eliminate pathogens or prevent their growth. Immunity in the HIS is basically structured around white blood cells and is divided into three categories [57]. Physical immunity provides the immunity at the skin level and at other physical barriers. The next set of immune strategies is called the Innate immune system, which are non-specific and quick to act. Responses such as inflammation are due to these Innate Immune systems. Basophils, which are a part of white blood cells, tend to create these inflammatory responses using a nitrogenous compound called histamine. Adaptive immune systems are more specific and may take more time than the innate immune systems; however, they are more effective and try to identify the antigens specific to the cause. The adaptive immune system is activated by the dendritic cells which present the antigens to the antibodies or t-cells in some instances. This system can keep track of the attacks and is able to allocate some memory to identify the attacks. The adaptive immune system is further classified into humoral and cell mediated immunity. B-cells/B-lymphocytes are the key components of humoral immunity, which is an antibody specific immunity, since the B-cells are antibody producing cells which produce specific antibodies suited for specific antigens. When the dendritic cells present the antigens to the adaptive immune system, they produce a specific antibody which engulfs the antigen and present it to the T-cell or kill them by themselves. T-cells form the cell mediated immune strategy which tries to preempt the infected cells. While, B-cells kill the antigen from outside the cell, T-cells can enter the cell and kill the cells infected. B and T cells are further classified as killer cells and memory cells based on their properties such as memory and elimination. Both the T-cells and B-cells have the ability to distinguish between the external pathogens and the body’s own cells through a principle called

’self and non-self’. As the name suggests, pathogens are classified as self and the body’s cells are nonself. This differentiation allows the T and B cells to act against the non-self entities. The lymphatic system, which consists of organs, such as the spleen, lymph nodes, thymus and bone marrow, helps in producing and nurturing these immune specific cells.

As mentioned earlier, each leucocyte has a different role. For instance, basophil and eosinophils are the cells responsible for innate response. B and T cells are the important cogs of the adaptive Immune system as mentioned above. Dendritic Cells act as a link between innate and adaptive immune systems and present the antigens to the antibodies secreted by B cells. A detailed classification of Leucocytes is given in Fig. 4.2 The work in this dissertation, is mostly centered around Dendritic, B and T cells.

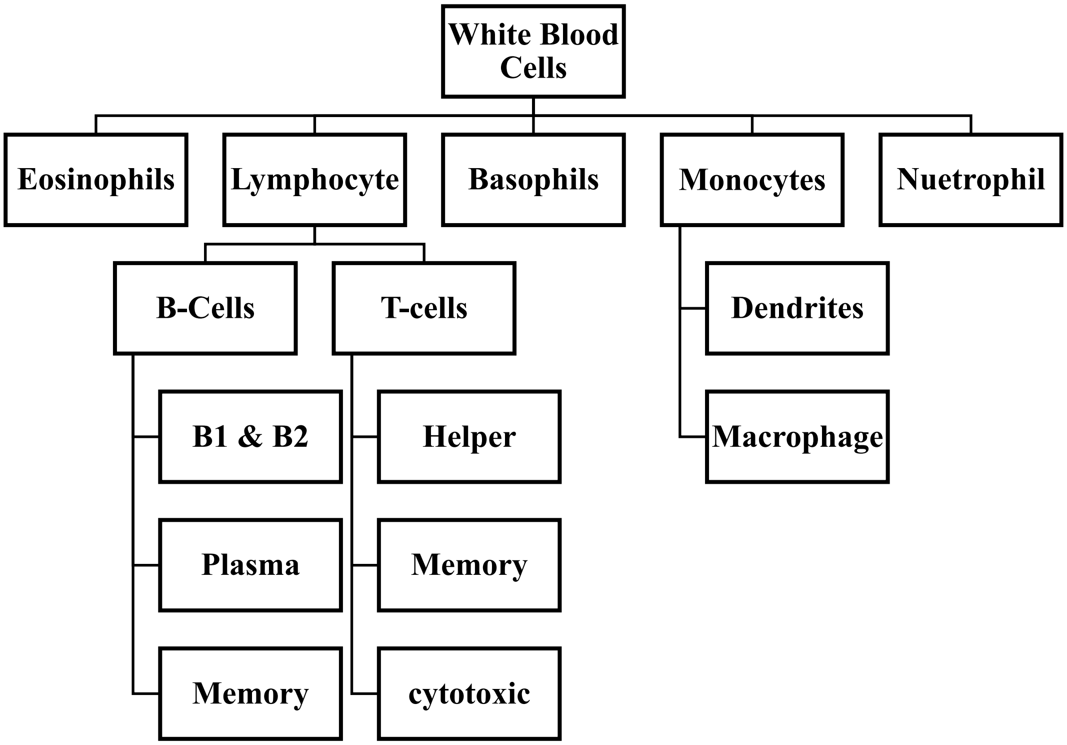


Figure 4.2 Classification of White Blood Cells

Table 4.1 Components of AIS

Entities	**Description**
Antigens	External stimuli that can excite the immune system
Antibodies	Protein, generated in response to an antigen.
B-cells	helps antibodies to counter antigens
T-cells	Kills or controls infected cells.
Bone-marrow	Produces immune cells.
Spleen	Stores immune cells.
Thymus	Maturation phase of T-cells.
Dendritic cell	Presents the antigens to antibodies.

4.2 Immune Theory Based IDS's

4.2.1 Danger Theory

The Danger model states that the tissues and cells are responsible for immune response when they are subjected to stress or abnormal cell death [58]. These tissues generate different kinds of danger or alarm signals after they identify an antigen presence. The signals generated generally include Damage-associated molecular patterns (DAMP) and pathogen associated molecular pattern (PAMP). Safe signals are also introduced to make sure there are no major false positives that might disrupt the functioning of the network. Although this model has both its merits and demerits when compared to the classical self and non-self model, Danger theory is generally more preferable to serve as a model for an Artificial Immune System for WSNs owing to its centralized organization and the low number of false positives.

4.2.2 Negative Selection

The Negative Selection Algorithm (NSA) is the most popular immune theory. It involves a random generation of detectors based on self and non-self models [16]. These generated detectors are then used to detect a non-self entity or an antibody. Biologically, a T-cell regulates a self- cell, if it finds one in the thymus and performs immune support during the maturation phase.

4.2.3 Positive Selection

Positive selection [19], as the name suggests, is strictly a reversal of the negative selection algorithm and is also not as popular as the NSA. The censoring is done to eliminate the non-self entities and the self-entities are used as the detector set. The ratio of the self and non-self strings determines which method to use among the negative and positive selection methods.

4.2.4 Clonal Selection

During the maturation phase of a B-cell by turning into a plasma cell, it undergoes mitosis and tends to divide and produce clones. This proliferation takes place only when the B-cell binds to the external pathogen or antigen and can identify it [59]. These clones are not entirely identical due to hyper mutation. This process is done in two stages. The first stage ensures the antigen binding antibodies convert into B-cells and the second stage is the cloning phase. This helps to nullify the non-self space.

4.2.5 Hybrid

Although immune principles such as negative selection and clonal selection go hand-in-hand, these theories can also be used in conjunction with other existing anomaly detection methods. That is, a hybrid model is a combination of the conventional intrusion detection systems and the immune inspired detectors. NETRIIAD [60], a hybrid intrusion detection mechanism tries to combine the danger theory inspired immune techniques to the conventional signature analysis techniques. The alerts produced by using a misuse-based detector are passed on as danger signals into the network and the corresponding weights and concentrations are calculated. The output calculated defines whether there is any intrusion in the network. The author comments that this technique is more effective than the conventional misuse-based techniques.

4.2.6 Network Based Models

As the name suggests, a network of nodes analogous to the B-cells, T-cells or a cluster of different types of immune cells form a wireless network [61]. The properties of these nodes are defined by the properties of their corresponding immune cells. Each node is assigned a specific task similar to its counterpart in the human immune system. For example, AINE [62], [63] uses an artificial recognition ball (ARB) to create an AIS through a network of B-cells using the clonal selection principle. The initial set is cloned to get a second set of population. A network affinity threshold (NAT) is used to create the links in the network. Recognition ball is the region which is supposed to aid the antibodies to detect antigens. Methods such as IBM’s virus detector are some of the early works based on network-based models.

4.2.7 Others

1) CARDINAL: Cooperative Automated Worm Response and Detection Immune Algorithm, which is abbreviated as ’CARDINAL’ [64] is inspired by the immune properties of the T-cells;

more specifically, the differentiation states of T-cells. A strict duplication of the T cell maturation process is used in a network to detect and respond to external threats.

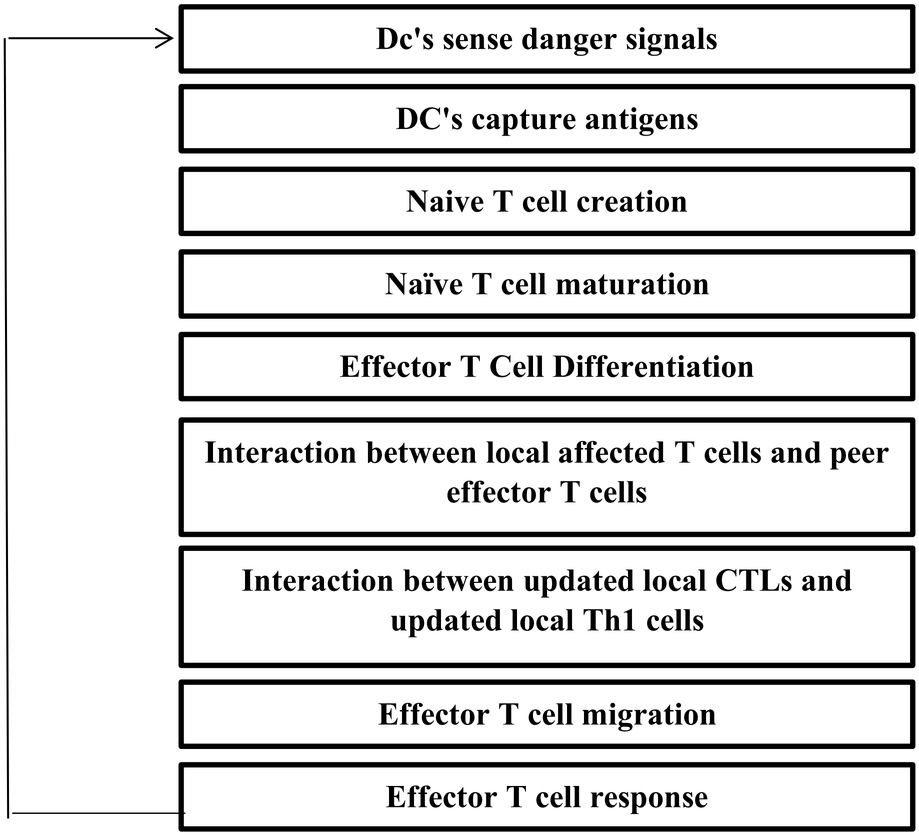

Dc's sense danger signals
DC's capture antigens
Naive T cell creation
Naïve T cell maturation
Effector T Cell Differentiation
Interaction between local affected T cells and peer effector T cells
Interaction between updated local CTLs and updated local Th1 cells
Effector T cell migration
Effector T cell response

Figure 4.3 Flowchart of CARDINAL

2) Machine Learning: In this model, machine learning is used to classify whether the data is anomalous or not [65]. After this classification, a set of virtual antibodies are being generated by the cluster heads (Aggregator and control node for a cluster of WSN's) and passed on to the sensor nodes in the network. These antibodies, based on the trust rating generated by the networks sink node, disable the nodes with any fraudulent activity.

3) Co-FAIS: Co-FAIS [66] or Cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks introduces a parameter called context antigen value to monitor the abnormality in the network's traffic and instigates a fuzzy misuse detector module (FMDM) and a

fuzzy Q-learning module by updating the fuzzy activation threshold. The outcome from the misuse detector module, in turn prompts the cooperation decision making module. This module determines which detection module to use based on an analysis of the attack and the source of attack. A response module is triggered after the detection. Table 4.2 summarizes the Danger theory, Clonal Selection, Negative selection and Positive Selection mechanisms and highlights a few similarities and differences.

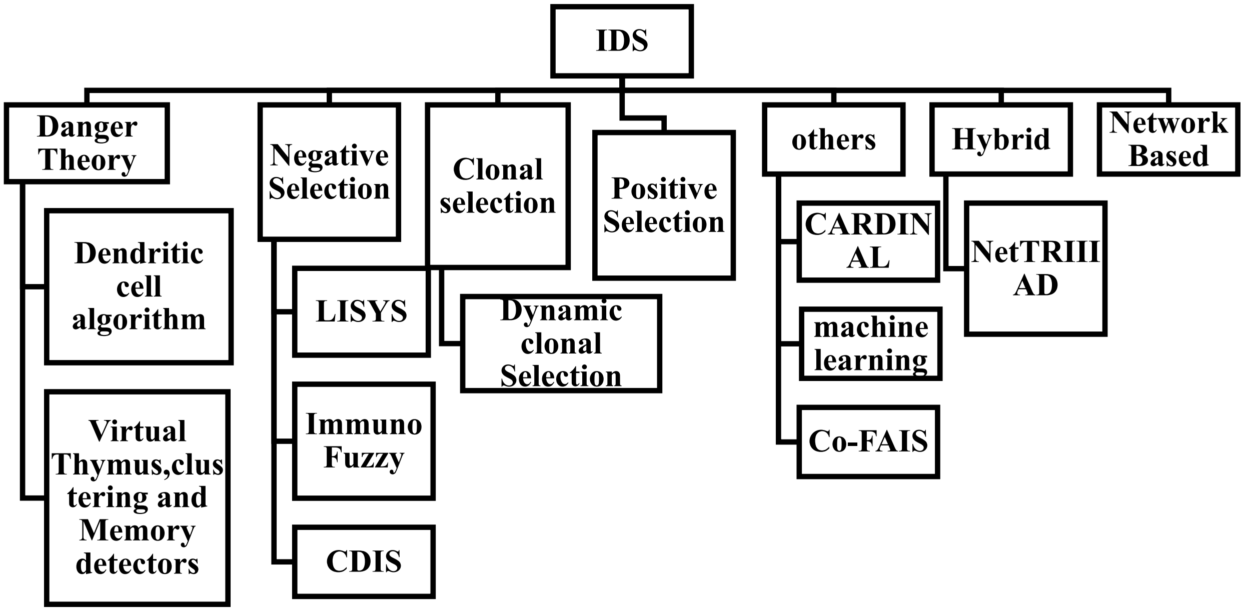


Figure 4.4 Immune Based Intrusion Detection Systems

4.3 Applicability to WSN's

4.3.1 Danger Theory Applicability to WSN's

An Intrusion Detection system designed based on danger theory need not focus on representing a set of data; however, it can be used as a mechanism to determine which data to focus on [67]. Wireless Sensor Networks are generally energy constrained and transmit significant amounts of data through numerous nodes; therefore, they are prone to a wide variety of attacks and loss of resources as mentioned in chapter 1. Anomalies in resource allocation, resource transfer and any noticeable or abnormal changes in the network functioning can be termed a danger signal. Examples of these signals are:

- Too high or too low memory usage
- Too high or too low energy consumption
- Unexpected frequency of data transfer
- Abnormal termination of a node
- Non-repudiation

The Intrusion detection process can be activated and deactivated at any instant of time, enabling the sensor network to save more resources. Fig.4.5 shows a danger signal generated when an anomaly is detected. The source wants to send the data to its destination; however, it receives no acknowledgement from node ’D’.

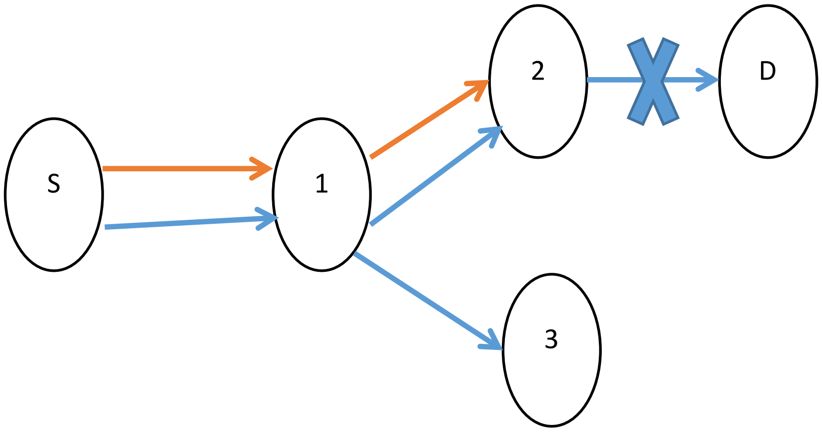


Figure 4.5 Transmitting a Danger Signal

Hence, it sends a danger signal along the path traveled to reach its destination via node 1 and node 2. Here, node 2 is the affected node which drops the packets. A danger signal is delivered after an anomaly is detected. All the signals generated are collected, weighed and the impact is calculated. Due to this nature of the detection algorithm, a low number of false positives are an added advantage.

1) Dendritic Cell Algorithm: Dendritic cells are subjected to a volume of signals which classify them as mature or semi mature. This classification helps in determining the safe or unsafe state of a network. Greensmith et al. [68] categorized DC input signals into four groups PAMPs (signals known to be pathogenic), Safe Signals (signals known to be normal), anger Signals (signals that may indicate changes in behavior) and Inflammatory Cytokines (signals that amplify the effects of other signals). Cytokine signals further try to organize the T cells into helper and killer T cells. The weights of these signals are calculated, and an anomaly is detected. Kim et al. [69] used a sensor network attack called Interest Cache Poisoning and generated six types of signals. As mentioned earlier, danger signals are generated to alert the system of any changes in resources, such as packet insertion rate and cache entry expiration. A safe signal is generated showing that the network is in normal state at that instant. A pathogenic signal shows a failure or an anomaly.

$$Output\ Cytokine = C_{[csm,semi,mat]} = \frac{(w_p * c_p) + (w_s * c_s) + (w_d * c_d)}{|w_p| + |w_s| + |w_d|} * \frac{1 + IC}{2} \tag{4.1}$$

2) Using Virtual Thymus: This method of Intrusion detection uses the antigens observed along with the danger signals [70]; therefore, it forms two layers of detection without the need for a preliminary learning mechanism. Memory detectors are used to achieve the two-layered approach by providing a swift secondary response. Virtual Thymus is the AIS used to detect an anomaly. It acts as the central processing unit and correlates the danger signal to the observed antigens.

4.3.2 Negative Selection Applicability

As mentioned above, negative selection is based on the concept of self and non-self. The censoring part of the NSA tries to generate a number of random binary strings and then compare these with self-strings. The strings that get matched as self are discarded and the rest are labeled as a detector set. This detector set is used to match the strings in the network during the detection phase and are labeled as an anomaly or non-self, if there is a match. Unlike danger theory, negative selection is bound to have a considerable number of false negatives due to the fact that it does not possess a centralized risk weighing mechanism and has a comparatively inconsistent memory detector mechanism. Also, negative selection is not suitable for a densely populated environment or a network with heavy traffic. As the traffic increases, the number of detector sets increases. Since the detector set is randomly generated, it increases the latency and becomes computationally inefficient. The two stages of the negative selection algorithm are shown in Fig.4.6 and 4.7 [71].

1) LISYS*:* LISYS [72] is designed as a light weight detection system to be operated in a local area network using r-contiguous bit matching. The self and non-self parameters are determined by the traffic flow between the nodes. The information is compressed in set of 49 bit strings. A set of detectors are also derived using the same 49 bit string format [73]. A negative selection algorithm is implemented by using a set of detectors derived from r-contiguous bit matching [74]. This rule states that two strings need not be identical in all the locations of a string. They can be matched if they are similar in at least ’r’ contiguous locations.

2) Immuno Fuzzy: The Immuno Fuzzy technique uses the negative selection algorithm with a set of fuzzy detector rules. This work is characterized by the use of hyper rectangles to represent the data in the network. Gomez et al [75] used fuzzy rules to a non- self space as detection rules and

determined if the data is self or non-self. The authors claim that the usage of a fuzzy detector set brings accuracy and dependability to the system.

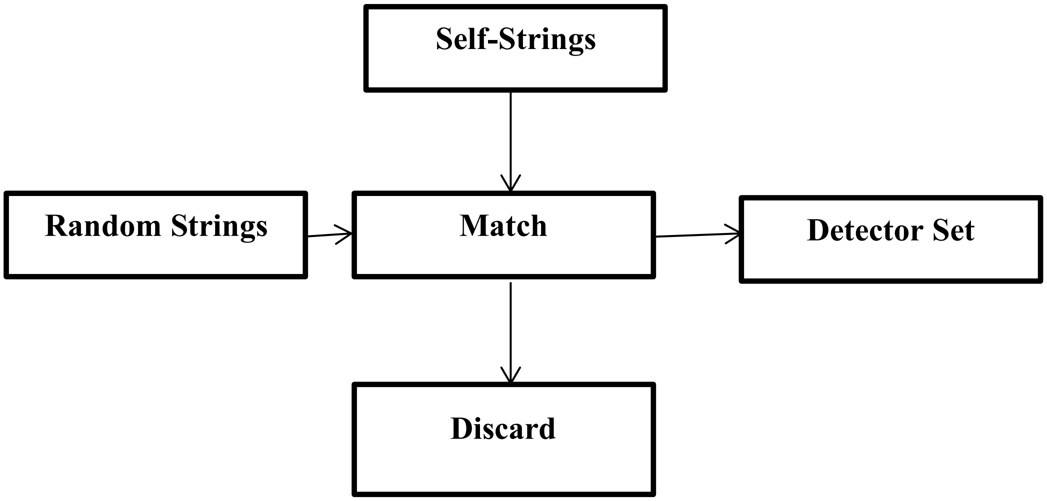


Figure 4.6 Censoring

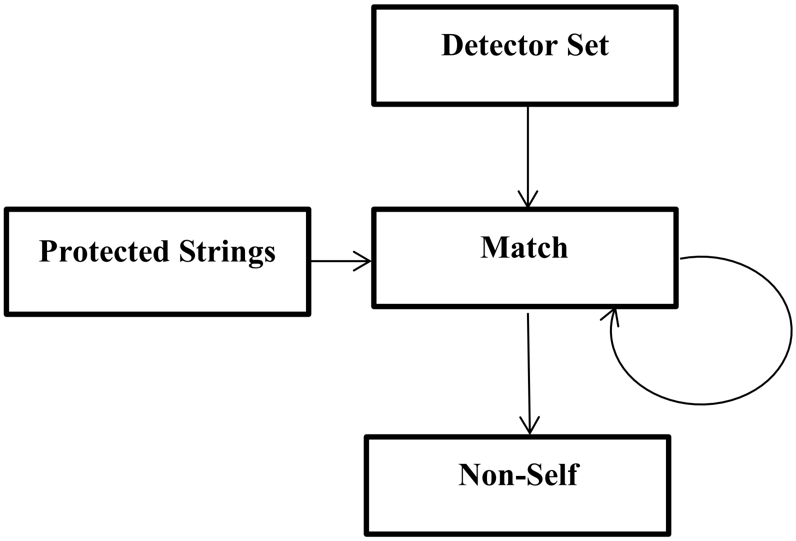


Figure 4.7 Detection

4.3.3 Clonal Selection Applicability

Clonal selection is usually employed in conjunction with a negative selection operator or an affinity calculator, which is used to calculate the affinity between the antibody and the antigen. The detector set formed from the negative selection algorithm is cloned and a set of identical clones are generated. These clones, however, are not entirely identical. Hyper mutation ensures that the clones generated are of varied forms of the parent clone but are of the same string size. This has the effect of making the detector set larger and more comprehensive.

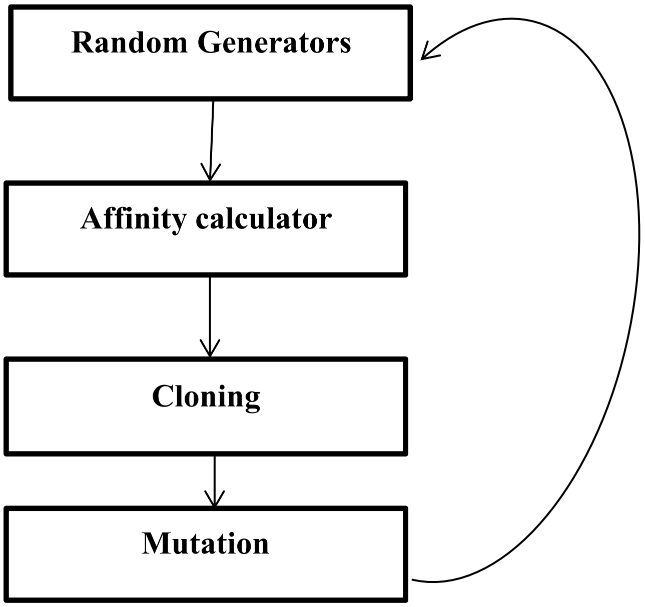


Figure 4.8. Clonal Selection

1) Dynamic Clonal Selection:'DynamiCS' [76] introduces some new parameters to the detection system.

- 'Toleration period' to specify a necessity of a new antigen set.
- 'Life span' to detect and delete the matured detectors after a pre-defined life span.
- 'Activation threshold' to generate a memory detector.

Table 4.2 Comparison of Immune Based IDS

Danger Theory	**Clonal Selection**	**Negative Selection**	**Positive Selection**
Suitable for dense Environments	Not suitable for dense environments	Not suitable for dense environments	Not suitable for dense environments
Low false positives	High False Positives	High False Negatives	High False positives
Can cope with the change of network dynamics.	Cannot cope up with changing dynamics.	Cannot cope up with changing dynamics of the system with respect to time.	Cannot cope up with changing dynamics.
Can work without memory detectors	Memory Detectors	Memory Detectors	Has Memory Detectors
Constant response time.	Faster response time, when used with negative selection.	Faster Response time, but induced latency can be observed.	Faster response time.
Centralized	Distributed	Distributed	Distributed
Degree of damage can be deduced.	Degree of damage cannot be inferred instantly.	Degree of damage cannot be inferred instantly.	Degree of damage cannot be inferred instantly.
High depth of Detection Capability (number of attacks patterns known or learned)	Considerable depth of Detection Capability	High depth of Detection Capability	High depth of Detection Capability

CHAPTER 5: ENGINEERING AN ARTIFICIAL IMMUNE SYSTEM

5.1 Danger Theory Based AIS

The IDS developed will be studied in three phases. While the first phase includes drawing an analogy using different leucocytes, assigning node functionalities and giving an overview of the system, the second and third phases include establishing the innate and adaptive response systems, respectively. While Fig. 5.1 demonstrates the second and third phases of the system through a flow chart, Fig. 5 .2 gives an illustration of the first phase, which adapts the immune cell properties into a wireless sensor Network. Each corresponding node adapts the designated immune properties of these cells. For instance, a Dendritic cell is mapped to a detection node which has a higher priority than the other nodes. Similarly, we have a B-cell and a T-cell mapped to certain nodes in a WSN which are the part of the detection process and are designated to be the detection nodes.

5.1.1 Drawing an Analogy and Modeling the IDS

The IDS proposed is built around an immune model called Danger Theory. Dendritic cells act as a bridge between innate and adaptive immune systems and act as the immune cell responsible for activating immune response by sending alerts.

[3] Parts of this chapter were published in IEEE Access, 6, pp.47364- 47373,2018. Permission is included in Appendix A.

These alerts, in the form of danger signals and PAMP signals are exploited by correlating them with a handful of WSN features which are vital for the functioning of the network. Features such as energy, packets transmitted, and time duration are obtained, and a statistical change is noted for anomaly detection through the alerts. A few nodes mimicking specific immune cells are strategically placed in a cluster and certain tasks are assigned to each of those specialized nodes along with providing some computational abilities. These nodes, which are ideally placed close to root or sink nodes, include Dendritic, B, T and a Basophil cells. These nodes combine to create a private network in order to communicate among each other. Fig. 5.3 gives an illustration of this network which is the mainstay of the proposed AIS. As a part of the preliminary detection process or the innate immunity process, the network profile is synthesized as artificial peptides and fed to the B-cell, which tries to match them to the PAMP's generated as a part of the Adaptive immunity system discussed in the sequel. This phase is called PAMP Analysis, as seen in Fig. 5.1 and it helps in reducing the energy consumption of the IDS and also the time required to detect an attack. If an attack is not detected during this stage, it is turned over to the dendritic cell for further analysis. This stage is the Adaptive immunity phase, which generates the Danger signals and calculates the aggregator output to determine an Anomaly and is shown in Fig.5.1. The dendritic cell possesses the computational abilities to determine an anomaly and alert the network by sending danger and PAMP signals along with cytokine signals. The quantified signals are matched with their respective weights and an aggregator output is obtained. It should be noted that this aggregator output does not necessarily specify the extent of anomaly.

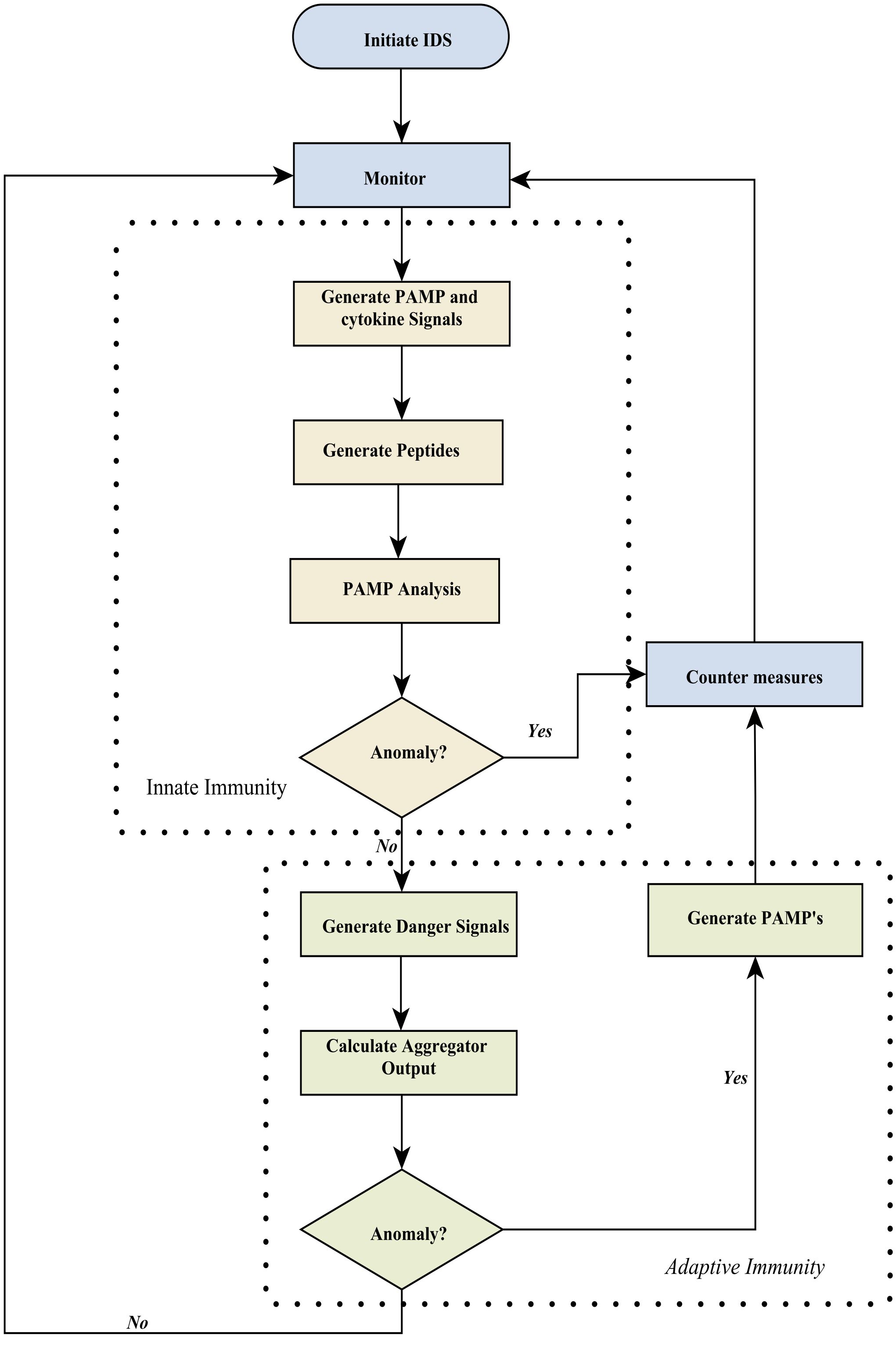


Figure 5.1 Flowchart of the IDS

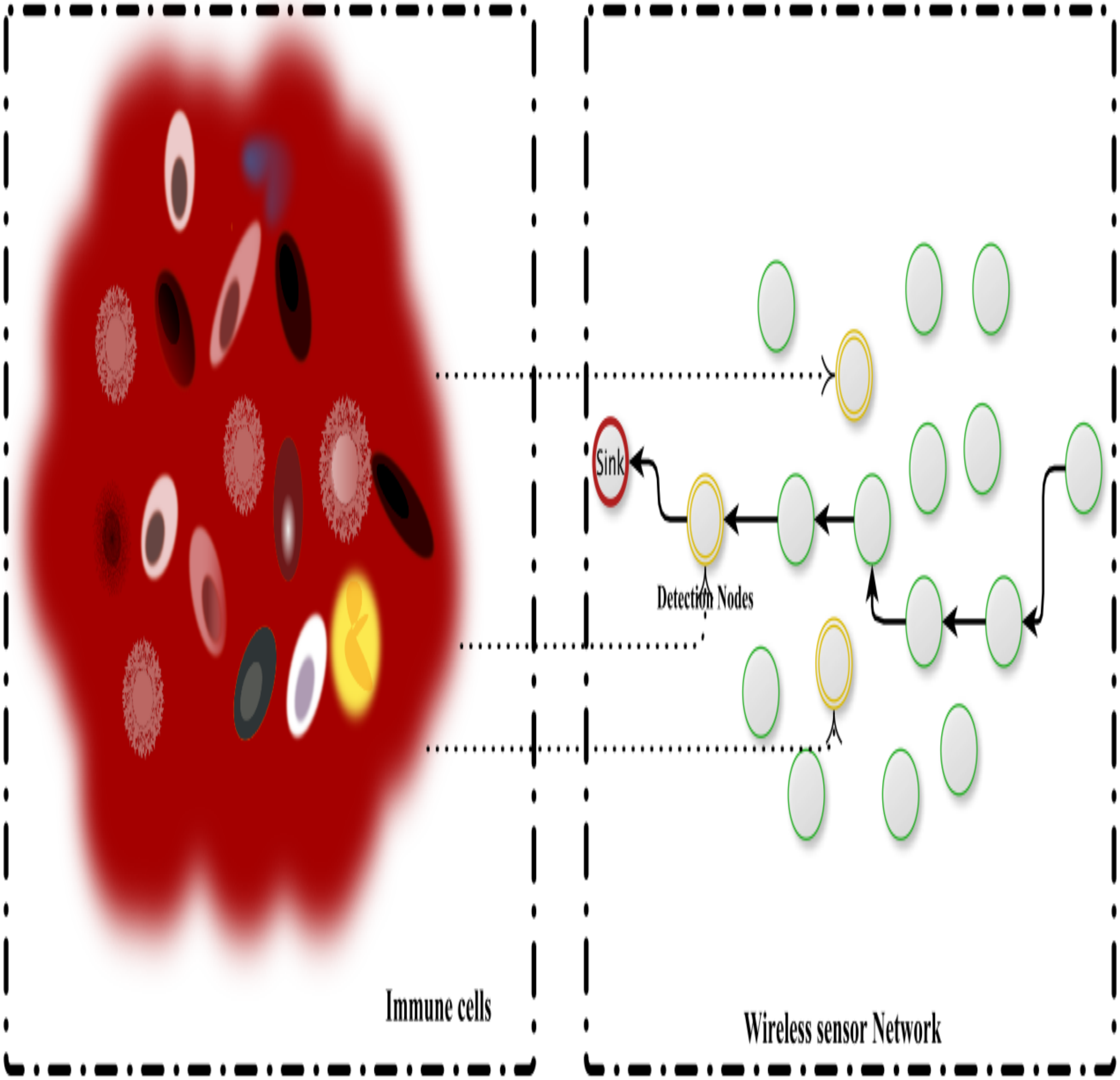


Figure 5.2 Deriving an Analogy from HIS to WSN

The aggregator output determines whether the node under test is sent to the basophil or the T node/cell. If the aggregator output is greater than the threshold (δ_1), an anomaly is noted. If the aggregator output is below the predefined threshold (δ_2), the node under test will be sent to the basophil which initiates and performs intrusion response. These response techniques can be generic or focused towards a particular type of attack. They can include limiting the data sent from the anomalous node, discarding redundant packets from the affected node, restricting the rate of transmission, use of various error correction techniques and barring connection requests from the malicious node. Basophil implementation is not studied in this work. If the aggregator output is greater than the threshold (δ_2), the node under test will be sent to the T node/cell, which shuts down or isolates the anomalous node and caches the information regarding the node in its own reserved memory which can be used for future analysis. B cell has its own reserved memory which contains the PAMPs that is, the anomalous signatures which are used for PAMP analysis using bit matching.

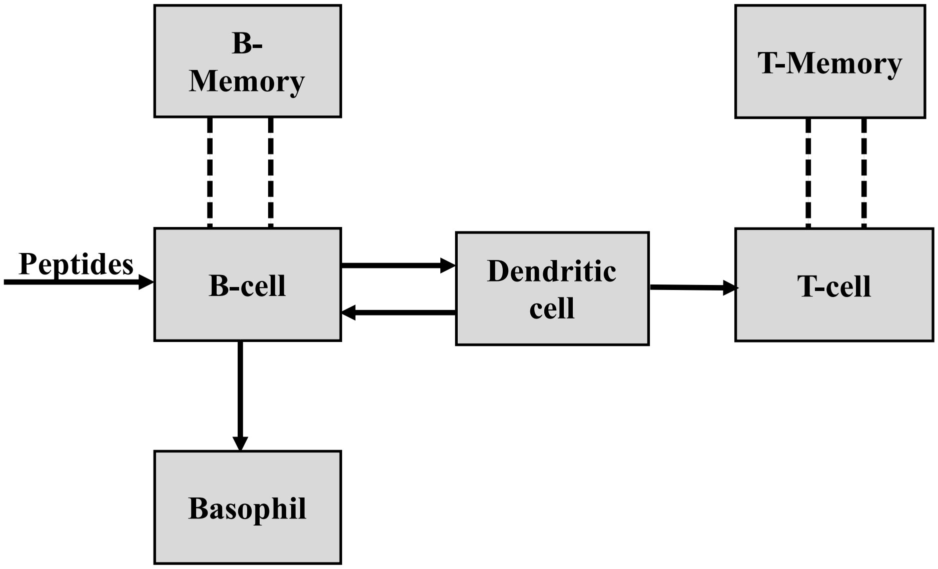


Figure 5.3 Block Diagram of AIS

A total of nine alert signals are generated out of which two of them are danger signals, three are PAMP signals, one is a safe signal, and the other three are cytokine signals. DS1 is the first danger signal and is based on probabilistic energy comparisons. Another danger signal (DS2) is generated when there is statistical anomaly in the data sent and received. PS1 is attained by monitoring the frequency of the data transfer from a particular node to the sink. PS2 is produced by looking at the duration of the connection each node has with its sink or the cluster head. PS3 is based on the time of transfer, rather the time interval between the transfers. Cytokine signals, IC1, IC2 and IC3 are derived based on the node status, number of hops and the type of connection respectively.

Type of connection (local/remote) is determined by monitoring whether the node is transmitting in the same cluster. Node status and type of connection are binary value representations during the detection process. A Safe Signal (SS) is also incorporated to make sure the network wouldn’t start responding for intrusion even when there is no intrusion. A safe signal is sent when the sink receives all the data it is supposed to, in a timely fashion. If a safe signal is received after the basophil initiates intrusion response, it triggers immunosuppression, which means that the response mechanism is driven down. It should be noted that there can be more than one signal at any given instant of time. A cumulative output is determined by assigning weights to these signals resulting in the aggregator output. The weights of the signals are determined based on their impact on the network behavior and their likeliness to predict an intrusion. A graphical representation of these weights in a descending order is given in Fig. 5.4. Aggregator output, calculated based on the signals generated is given by equation 5.1.

$$\mathit{Aggregator\ Output} = \left|\sum_{ps1}^{ps3}\left(W_p * C_p\right)\right| + \left|\sum_{ds1}^{ds3}\left(W_d * C_d\right)\right| + \sum_{ic1}^{ic3} C_{ic} \tag{5.1}$$

$$W_{ds1} + W_{ds2} + W_{ps1} + W_{ps2} + W_{ps3} = 1 \tag{5.2}$$

Here, Wp, Wd and Wic represent the weights of the parameters used. C_p, C_d, C_{ic} are the concentrations of PAMP, danger and the cytokine signals respectively. The weights the system assumes are arbitrary. They can be varied and reconfigured during the execution. The rationale behind using the proposed weighing scheme is the impact of those features over the network performance and the number of false positives these parameters generate when they are used as a part of an IDS. So, effectively, the parameters with higher influence on the network's performance such as energy and data transmitted have higher weights. As mentioned earlier, these weights can be varied depending on the user requirements and the type of attack the system is typically prone to. C_p, C_d, C_{ic} are calculated based on the statistical analysis of the various danger and PAMP signals. Cytokine concentrations assume binary values as mentioned above and only appear in the integer part. A cytokine signal confirms an anomaly. When there are no cytokine signals, the fraction part will be the measure of anomalous activity. Concentrations, C_p and C_d are assigned values in the range of 0.1 to 1 with a step increase of 0.1. The signal outputs obtained will be sampled into multiple range of values and each range is represented with multiples of 0.1.

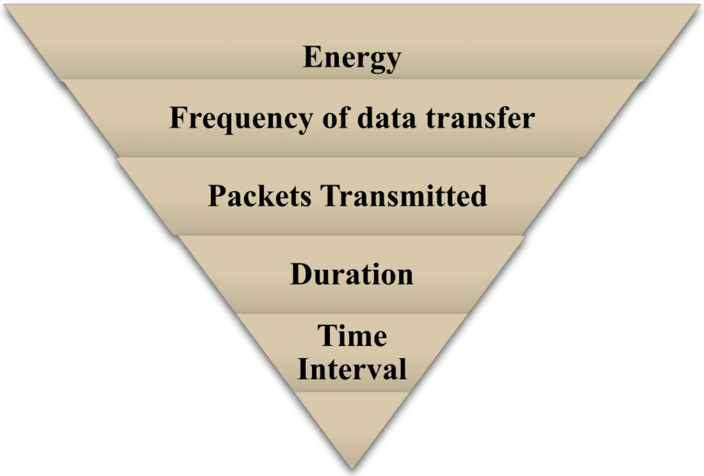


Figure 5.4 Weights of the Parameters from High to Low

5.1.2 Generation of Peptides and PAMP Analysis

A set of peptides are derived from each node on different time intervals. These peptides are then fed to the B-cells to perform PAMP analysis. PAMP's are the attack signatures that are derived previously and are stored in the B-memory. B-cell compares these artificial peptides to the PAMP's using a bit matching algorithm and certifies an intrusion when a match is found. The peptides derived based on network profile are in the form of binary strings and have a length of 121 bits. The order of the string would be source address, destination address, duration, time interval, bytes received, bytes sent, Hop Count, protocol type, Connection type and node status. A typical peptide would look like (e,1, 6, c,7, a, c, e, 1, 6, c, 7, a, 1, 2, 0, 0, 0, 7, 6, 5, 7, 0, 0, 0, 2, 4, 5, 6, 0, 0, 8, 9, 0, 1, 2, 1, 5, 7, 1, 1). The string contains the information that the source address 225.108.122.12 is sending and receiving 2456 and 7657 bytes respectively to and from 225.108.122.12 for a duration of 86 seconds with a hop count of 5. The last couple of binary representations mean that the node is transmitting locally and to an active node. If a match is found for this peptide, in the B-memory, then it signals an anomaly. The Algorithm 5.1 below gives an overview of a version of PAMP analysis and the subsequent detection process.

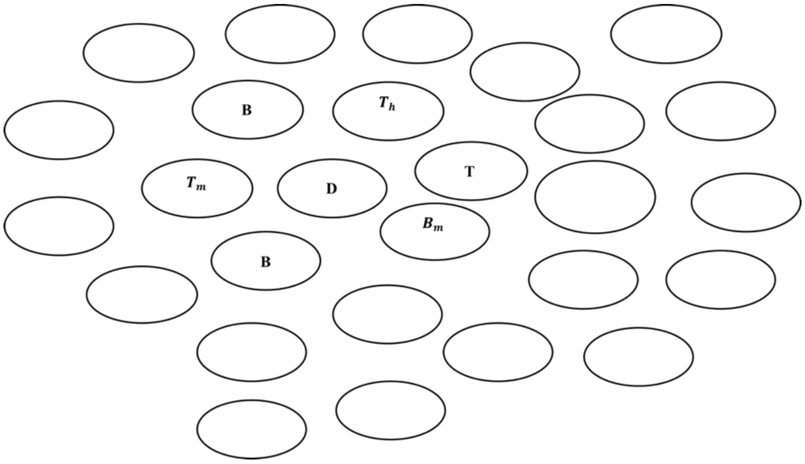


Figure 5.5 An Immune Mediated Wireless Cluster

Algorithm 5.1 PAMP Analysis & Consequent Steps

```
Input:  Artificial Peptides,
Output: Aggregator Output
Result: Intrusion detection.
while $Source_{pe} = Source_{pa}$ && $Destination_{pe} = Destination_{pa}$ do
    if $PS_{pe}=PS_{pa}$ || $IC_{pe}= IC_{pa}$, then
        confirm Intrusion
    else compute Aggregator Outputs
        while ($AO > \delta_1$) do
            Confirm Anomaly
            if ($AO < \delta_2$) then
                Send to Basophil for response
            else Send to T-cell
            end if
        end while
    end if
end while
```

5.1.3 Generating Danger and PAMP Signals

Anomalies in energy consumed are obtained based on the difference between the predicted and the residual energies. Probabilities of state transitions between sensing, calculating, sending, receiving and sleep modes are determined by using Chapman-Kolmogorov equations [77] based on Markov chain modelling [78]. Fig 5.5 gives a state transition diagram of the system. The system assumes a Markovian process, when the probability of transitioning from one state 'i' to the next state 'j' is not dependent on any other states, which are in operation prior to the preceding state 'i'. When a sequence of random variables, $\{x_1, x_2, x_3, x_4, x_5, \ \ldots\ldots\}$, which denote the state of the network satisfy the Markovian process, along with assuming the properties $P_{\mathrm{ij}} = 0$ and $\sum_{\mathrm{j}=0}^{\infty} P_{\mathrm{ij}} = 1$ they are said to adopt a Markovian chain. Chapman-Kolmogorov equations can be realized when the network or a system which satisfies the Markovian property and follow a finite discrete time process. These equations can help determine the probability of the system to move from one state to another in 'n' time steps. Using these equations, the probability of state transitions from i to j in 't' time slots is given in equation (5.3),

$$P_{ij}^{t} = \sum_{k=0}^{t} P_{ki}^{r} P_{kj}^{(t-r)} \qquad (\, 0 < \mathrm{r} < \mathrm{t}\,) \qquad (5.3)$$

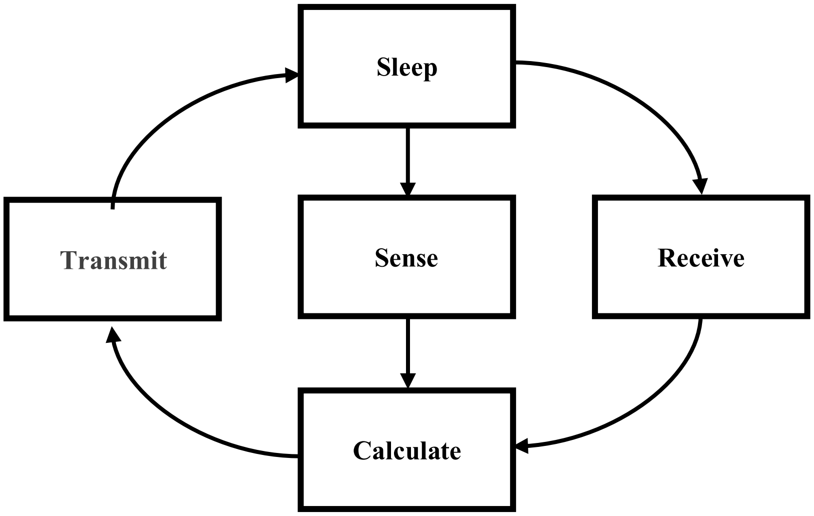


Figure 5.6 State Diagram of a WSN

where i is the initial state of the sensor node and j is the state of the node after ‘t’ time slots. By determining the initial state of the node under test, we can effectively deduce the node’s current state in its succeeding iterations. Before predicting the energy dissipated, the time slots the node remains in state j will be determined using the expression,

$$T_j = \sum_{t=1}^{T} P_{ij}^{t} \tag{5.4}$$

If we consider that the energy consumed at each time step as E_t, the energy predicted, E_p can be calculated by using

$$E_p = \sum_{j=1}^{5} (\sum_{t=1}^{T} P_{ij}^{t}) * E_t \tag{5.5}$$

The concentration of DS1 is obtained by calculating the difference between the energy predicted and the actual energy consumed, i.e.,

$$E_a = (E_i - E_r)$$

$$\mathrm{C}_{\mathrm{ds1}} = \frac{\left|(\mathrm{E}_{\mathrm{i}} - \mathrm{E}_{\mathrm{p}} - \mathrm{E}_{\mathrm{r}})\right|}{\mathrm{E}_{\mathrm{p}}} *\mathrm{n} \tag{5.6}$$

Here, E_i is the initial energy E_a is the actual energy and E_r is the residual energy of the node under test.

For DS2, data sent and received are predicted based on (5.3) and by determining the probabilities for state transitions to both sending and receiving states. The number of time slots the node will remain in receive and transmitting state is calculated using the following expressions:

$$\mathrm{T}_{\mathrm{pr}} = \sum_{t=1}^{T} P_{ir}^{t} \tag{5.7}$$

$$\mathrm{T}_{\mathrm{ps}} = \sum_{t=1}^{T} P_{is}^{t} \tag{5.8}$$

Here, *ir* and *is* are the changes of states to receive and send phases respectively. The sent and received packets are predicted using the formulas below. SP_p and RP_p are the predicted sent and received packets. SP_t and RP_t are the packets transmitted for each time slot.

$$SP_p = \sum_{j=1}^{3} (\sum_{t=1}^{T} P_{is}^{t}) * SP_t \tag{5.9}$$

$$RP_p = \sum_{j=1}^{3} (\sum_{t=1}^{T} P_{ir}^{t}) * RP_t \tag{5.10}$$

Concentrations of DS2 are determined by using the next expression, which is a result of comparison with the actual packets transmitted and the packets predicted to be transmitted.

$$\mathrm{C}_{\mathrm{ds2}} = \frac{\left|(\mathrm{SP}_{\mathrm{p}} - \mathrm{SP}_{\mathrm{a}}\right|}{\left|(\mathrm{RP}_{\mathrm{p}} - \mathrm{RP}_{\mathrm{a}}\right|} *\mathrm{n} \tag{5.11}$$

PS1 is determined by calculating the difference in the frequency of data transfers in 't' time slots.

$$C_{ps1} = \frac{\left| ft_t - ft_{th} \right|}{ft_T} * n \tag{5.12}$$

C_{ps1} can be calculated either by comparing the frequency of data transfer against a threshold or by comparing it with the frequency of transmission at earlier timeslots usually through statistical average. C_{ps2} and C_{ps3} can also be calculated in a similar way. It should be noted that the danger signals are not calculated at each collection point to avoid excess energy consumption.

5.2 Negative Selection

5.2.1 Modeling the IDS

As opposed to the IDS inspired from danger theory, the negative selection-based IDS need a training set of data prior to the actual functioning of the IDS. That is, the system is trained with the self and non-self-behaviors beforehand. Also, the detection process in danger theory-based IDS focused mostly on the system resources, the negative selection-based IDS only uses the features of the network such as time duration, time interval etc. In this system, the probable attack profile is fed to the detector nodes. These patterns are similar to the antibodies in an immune system. The process of modelling a negative selection-based IDS involves four stages.

During the first stage, the self-space or the normal patterns of the network are obtained through Contiki simulations which are discussed in the later parts of the paper. During the second stage, a set of random detectors are generated. All these profiles are converted to bit strings through the process similar to the one employed for danger theory-based IDS. The Euclidean distance between the strings of the self-region is determined and whenever there is a string match, that is an Euclidean distance of zero, the string is eliminated. This process helps in the elimination of redundant patterns. The maximum value obtained in this process is noted as S_{max} and is determined by the equation below.

$$\in_{s\,.} = \mathrm{sqrt}\,(\textstyle\sum_{i=1}^{n}((\,s_i - s_{i+1})^2 + (s_i - s_{i+2})^2 + \ (s_i - s_{i+3})^2 + \cdots \dots \dots (s_i - s_n)^2) \qquad (5.13)$$

The next step would be to determine the Euclidean distance from the self-strings to the detector set. The strings in the detector set which are closer to the self-set are eliminated and the rest of the strings are subject to further classification. The minimum value, d_{min} obtained for each detector is used to determine the antibodies. If the minimum Euclidean distance from a detector to the self-set, d_{min} is greater than $\alpha * S_{max}$, the detector is promoted as an antibody. α is a arbitrary parameter, which can be varied from 0 to 1.This process is continued in a loop until an ideal number of antibodies are generated. The distance calculated between the self and non-self-patterns (detector set) is given by the equation below.

$$\in_{d,s} = \sqrt{\ (\,(d_1 - s_1)^2 + (d_2 - s_2)^2 + (d_3 - s_3)^2 + (d_4 - s_4)^2 \dots \dots \dots . . (d_n - s_n)^2}) \qquad (5.14)$$

During the final stage, the attack patterns from the danger theory-based IDS can also be added to the detector set as antibodies. This requires a redundancy check, again. The antibodies which are stored as a detector set are used to compare and evaluate the network traffic for antigens, that is attack induced patterns. This process can be done using a bit matching technique or by employing the same Euclidean distance method used while training. Some IDS’s for computer networks also use a scheme called V-detector [79]. Since we are using WSN’s to build an IDS, we choose to go with an r-bit contiguous matching technique [8]. In addition, Euclidean distance can also be employed in conjunction with bit matching when the necessity for detection is high and the network overhead is not significant. The training is done such that it can adapt to both the techniques while the antibodies try to detect the antigens. IDS’s which are based on negative selection, normally use a function called fitness value or detector fitness to promote a detector as an antibody [81]. If the fitness of the antibodies is greater than the threshold, those detectors are restored as antibodies. In this work however, fitness level is calculated based on the efficiency of the antibody in detecting an attack during the testing process. The antibodies with low fitness value are termed as self-set and is discarded.

The detectors are derived based on network profile are in the form of binary strings and have a length of 92 bits. The order of the string would be source address, destination address, duration, time interval, bytes received, bytes sent, hop count and protocol type. These features are similar to the ones used in danger theory-based IDS. However, the string used here is binary as opposed to the real value representation in danger theory-based IDS. Although there are a few more features that can be taken into consideration while designing an IDS for WSN's using negative selection, this research is confined only to a certain set of features to bring out a consistent comparison between the danger theory-based IDS and the negative selection-based IDS. This scaling down of features also helps in reducing the computation power and memory requirements. Also, more antibodies can be produced if the system undergoes mutation of the acquired antibodies through clonal selection. However, the limited memory of a WSN node limits the number of antibodies that can be generated. At the same time, clonal selection is a very handy technique when an intrusion detection system is built for a computer network or a MANET.

Algorithm 2 Generating Antibodies

```
Input:  Self Set, Detector Set
Output: Antibodies            .
Generate a self-set
Calculate Euclidean distance of Self-set
if ($\in_s = 0$) then
    discard
else compute $S_{max}$
end if
Generate detector set
Calculate Euclidean distance of detector-set to self-set
if (($\in_d = 0$) then
    discard
else compute $d_{min}$
end if
if ($d_{min} < \alpha * s_{max}$)
    Store as Antibody
else discard
end if
```

5.3 Schizophrenic Nodes

A novel version of the attacks we discussed earlier is presented below and the performance of the IDS on these attacks is tested. The attacks are made time varying, that is the node turns malicious in random intervals and gains back its normal state during the next time slot. These nodes with time varying malicious capabilities are named schizophrenic nodes. The time slots follow uniform distribution [82] and the nodes turn back and forth from malicious to normal during each time step. Uniform distribution or rectangular distribution assigns equal probability to all the values in its range. The attacks which affect the schizophrenic nodes are blackhole, selective forwarding, flooding and wormhole.

$N_i = \{T_1, T_3, T_5, T_{7,} T_9, T_{11}, T_{13}, T_{15}..............\}$

$M_i = \{T_2, T_4, T_6, T_{8,} T_{10}, T_{12}, T_{14}, T_{16}.............. \}$

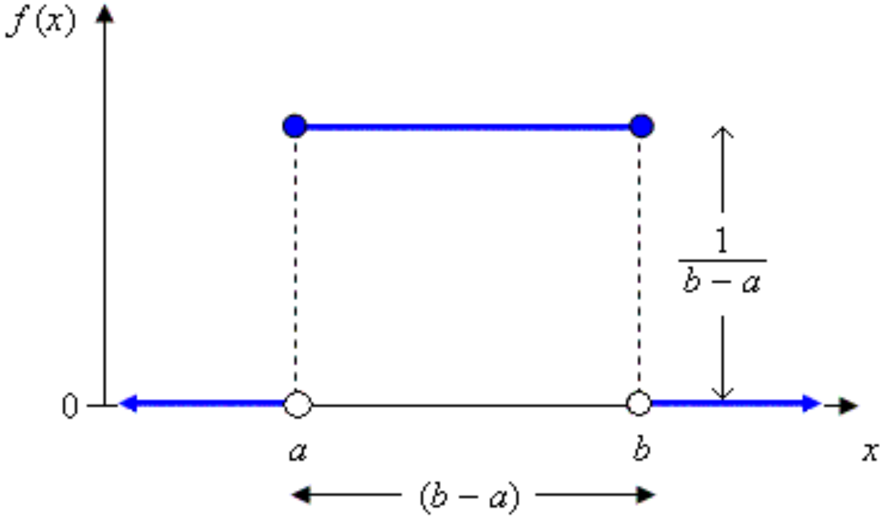


Figure 5.7 Probability Density Function

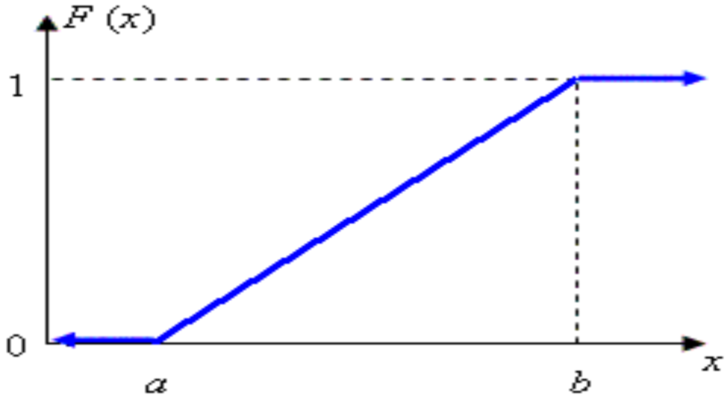


Figure 5.8 Cumulative Distributive Function

$$f(x) = \begin{cases} 0 & x < a \\ 0 & x > b \\ \frac{1}{b-a} & a \le x \le b \end{cases}$$

$$F(x) = \begin{cases} 0 & x < a \\ 1 & x > b \\ \frac{x-a}{b-a} & a \le x \le b \end{cases}$$

Here, N_i is the time slots when the node is under its normal operation. M_i is the set of time slots when the node turns malicious. P(x) and D(x) are the probability density function and cumulative distributive functions on the interval [a, b] respectively. As mentioned earlier, each time step is random and determined by subjecting them to uniform distribution. This makes the detection process more difficult and increases the latency. We employ such nodes in a WSN with RPL routing protocol and also test the effectiveness and the robustness of the danger theory-based IDS against these kinds of attacks. The time periods in the time slots are assigned a range of 1 to 30 seconds. Hence the probability density function of the distribution, in this case is 1/29.

CHAPTER 6: MODELING THE ATTACKS AND ANALYZING THE RESULTS

6.1 Modeling the Attacks

The effects and the nature of attacks are dealt with in chapter 3. Here, the discussion is about how four of those attacks are implemented and used in this dissertation. The attacks employed during this simulation are Blackhole, Selective forwarding, DDoS, and wormhole. These attacks are further categorized and implemented in various ways as shown below.

6.1.1 Selective Forwarding

Two types of Selective Forwarding attacks implemented in this work are packet delay based and packet loss-based attacks. While one attack buffers the packet at the anomalous node for a given period of time and transmits them after some time, resulting in a compromise in the freshness of the data, the other type of Selective forwarding attack implemented, discards packets at regular intervals.

6.1.2 Wormhole

A couple of different versions of Wormhole attacks are implemented based on the tunnel formed by the adversary. One of them creates a tunnel to a distant node in the same cluster, whereas the second variant creates a tunnel to a different cluster.

[4] Parts of this chapter were published in IEEE Access, 6, pp.47364- 47373,2018. Permission is included in Appendix A.

6.1.3 Flooding

DDoS attacks are implemented as control packet flooding and data packet flooding, both of them tend to overwhelm the network with excess and unwarranted information.

6.1.4 Blackhole

Three different Blackhole attacks are implemented by altering the placement of the malicious node in different ranks.

6.2 Routing Protocol for Low-Power and Lossy Networks

6.2.1 Routing Mechanism

RPL [83] works by making use of a set of Destination Oriented Directed Acyclic Graphs (DODAG's). All the nodes are assigned ranks based on their proximity to the sink node or the root. The nodes in the lower rank send information to the sink via the nodes in the upper rank otherwise called as parent nodes. As the name suggests, this protocol is suitable for low power and lossy networks such as wireless sensor networks.

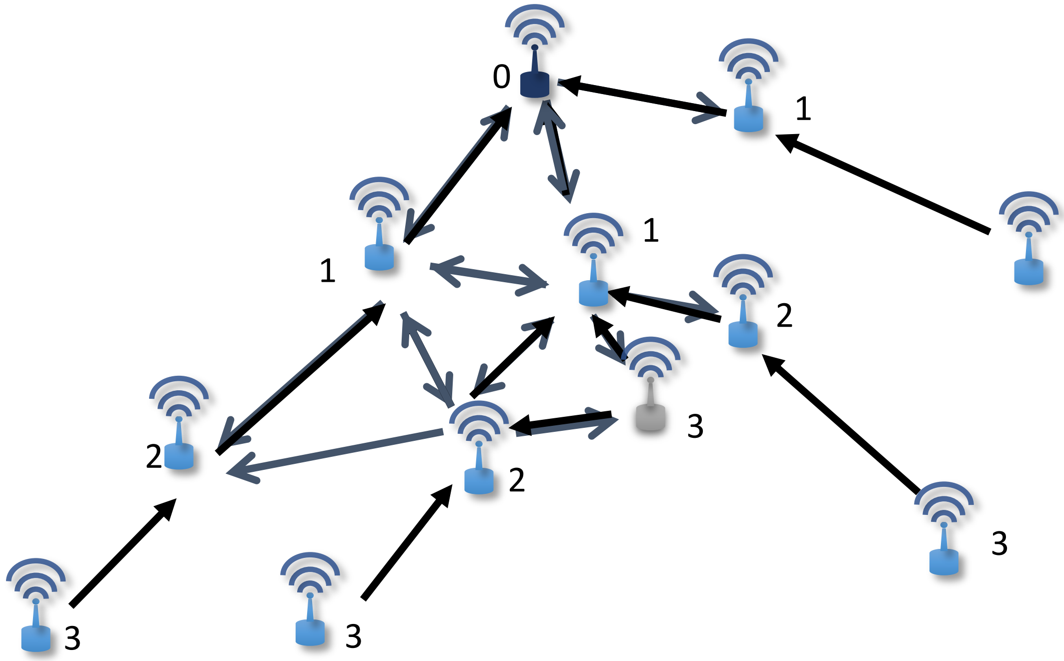


Figure 6.1 RPL Tree

The above figure gives an illustration of an RPL protocol. The nodes with rank 3 send data to the nodes in a higher rank, that is rank 2. The nodes in rank 2 in turn sends it to the nodes in rank 1, which is closest to the sink. The sink gets all its data from the nodes in rank 1.

All these nodes communicate through control messages, which are studied in the next section.

6.2.2 Control Packets in RPL

RPL has four control messages namely, DODAG Information Solicitation (DIS), DODAG Information Object (DIO), DODAG advertisement Object (DAO) and an Acknowledgement (ACK) to the DAO. DIO is multi casted to lower ranks by a specific node allowing those nodes to sniff the information regarding the multicasting node. DIO helps the lower ranked nodes in determining if they want to join the DODAG. DIS is sent when a node does not notice any DIO. DIS is broadcasted to see if any DODAG is available for the node to join. After the node finds a suitable DODAG either through acknowledging a DIO or sending a DIS, it makes a request to join the DODAG by sending a DAO. ACK is sent as an acknowledgement to DAO.

6.3 Simulation Setup

Simulations are done using a simulator called Cooja [84] in a Contiki environment using a protocol called RPL. 6LowPAN [85] and IPv6 are the protocols used at the network layer. RPL is a protocol to assist routing in low power and noisy networks.

During this simulation, the number of nodes deployed is varied from 20 to 30 to 40. The nodes are placed in a 100 m*100 m area with a range of 50 m. Simulations and calculations are performed to calculate the Aggregator output, detection rate, packet overhead and energy overhead for a danger theory-based IDS. The detection rates of the IDS are determined for the negative selection-based IDS. During the initial training phase, cytokine values under normal conditions are determined.

6.4 Analyzing the Results

6.4.1 Danger Theory

Table 6.1 gives an overview of the attacks implemented and the resultant anomalies quantified and expressed through danger and PAMP signals along with the Aggregator output. Fig.6.2 presents the Aggregator outputs of the attacks mentioned above, each of them individually simulated for a simulation time of 600 seconds. A preprocessed version of Fig. 6.2 with the alarm signals is given in Table 6.1. Both Table 6.1 and Fig. 6.2 are the resultants of an attacker in a 30-node network, the attack starting at 120 seconds. All the danger signals and PAMP signals calculated are presented in the form of percentiles during four time periods, T_1=240s, T_2=360s, T_3=480s and T_4=600s for all the attacks mentioned earlier. Blackhole attacks generate four different alarm signals, which are DS1, DS2, PS1 and PS3. Anomalies are found in energy, number of packets received or sent, time interval between transfers and the frequency of transfer. Since the three different Blackhole attacks are only a change in the location and RPL rank of the attacker node in the network and all the nodes are transmitting data at a uniform rate, the aggregator outputs do not show any significant variation from one another. There is a proportional increase in PS1 indicating that there exists an anomaly in the number of packets transmitted due to the aggregation of discarded packets as the time progresses. From Fig. 6.2, we see that the Blackhole curve has the highest output, when seen as a statistical mean of the aggregator outputs at different time slots, thereby it is easier to detect.

Wormhole1 generates DS1, IC2 and IC3. DS1 signal is due to the excessive energy used to forward a packet to a distant node which is exponentially larger than the energy used to send the packet to a neighboring node. IC2 is generated because of the change in the number of hops to the sink. IC3 is due to the connection being remote, that is the node is transmitting to a different cluster. Wormhole2 has similar signals compared to Wormhole1 except the cytokine signal IC3 since it is transmitting locally however with a change in the number of hops. The aggregator output for both Wormhole1 and Wormhole2 has an integer part unlike the rest of the attacks indicating a cytokine presence. As mentioned earlier, a cytokine presence concludes a definite intrusion. DDoS produces the highest final aggregator output.

Both the DDoS attacks witness a substantial anomaly in the energy consumed by the anomalous node. This is due to the flooding of the network and thereby depleting the already constrained resources. DDoS1 floods the network by repeatedly sending DIO's resulting in redundancy. Hence DDoS1 generates only DS1 and PS3. DDoS2 yields DS2 as opposed to DDos1 since it floods the network with UDP packets. Here, the anomalies are found in energy, packets transmitted, duration of the established connection and the time interval (DS1, DS2, PS2 and PS3). The aggregator output of DDoS from Fig. 6.2 moves past Blackhole at time T_4, showing that it is easier to detect DDoS attacks than Blackhole as the simulation time passes a certain threshold. Figures 6.3, 6.4, 6.5 and 6.6 show the aggregator outputs for blackhole, flooding, wormhole and selective forwarding attacks respectively. A more detailed comparisons of detection probabilities is given in Fig. 6.7.

Selective forwarding produces the lowest aggregator output value. This renders it harder to detect. This is due to the not very substantial change in the energy consumed. On the other hand, this may also be due to the low weights assigned to DS2. More reasons for this behavior are mentioned in the later parts of this work. Calibrating the weights can result in a better detection probability for Selective Forwarding attacks. However, this leads to an increase in the number of false positives to a considerable extent along with a change in the detection probabilities of other attacks. This is not a desirable trade-off. Both the variants of Selective forwarding attacks have the same signals associated with them (DS1 and DS2) and are comparatively difficult to detect using this detection method. It should be noted that even when some packet delay is associated with one of the attacks, there are no PAMP signals generated.

If we consider δ_1 as 0.1 and δ_2 as 0.3, the intrusion is detected for all the attacks except Selective Forwarding at the first detection point (T_1) and is sent to the basophil for countermeasures. However, this is not the case with Selective forwarding. The attack is not detected until the third detection point(T_3) before it is sent to the basophil. Only the nodes with DDoS and Blackhole after T_3 is sent to the T-cell. By varying the threshold, we can determine and set an intrusion tolerance level to all the nodes in the network. Fig. 6.8 and Fig. 6.9 provides the packet and energy overhead caused by the IDS respectively for 20,30 and 40 nodes, both of which are vital to the network functioning due to the constraints a WSN possesses. Probability of detection for each attack is derived against the simulated time. Detection rate is measured by varying the seed, placement strategies, number of attackers and as mentioned earlier, number of nodes. From Fig. 6.7, it can be inferred that Selective forwarding has the least detection probability from this approach. Along with the factors mentioned above, this is also due to the fact that quantum of the packets dropped is not as significant as Blackhole, which discards all the packets traversing through the malicious node and also relatively less energy deviations from the predicted results. Although the detection probability climbs up at a later time due to the aggregation in packets dropped, nevertheless it is lower than the other attacks.

DDoS has the highest detection probability and is one of the easiest attacks to detect using this model, since a noticeable change can be seen in the energy consumed and also since DS1 has the maximum weight among all the signals. Blackhole is another easily detectable intrusion and has one of the highest detection rates due to the number of packets it discards. However, the detection is not probability is not near perfect for a Blackhole attack because of the nodes which are located at a remote location and do not act as intermediate nodes or do not join the DODAG. Detecting an intrusion in these nodes is problematic. A Cytokine presence is typically traced for a Wormhole attack. However, even when there isn't a cytokine occurrence, Wormhole has a decent detection probability as evident from Fig. 6.2 and Fig. 6.7. The same scenario with the same attack is implemented twice to check the effectiveness of the B-cell. Iteration1 gives the results of the first experiment.

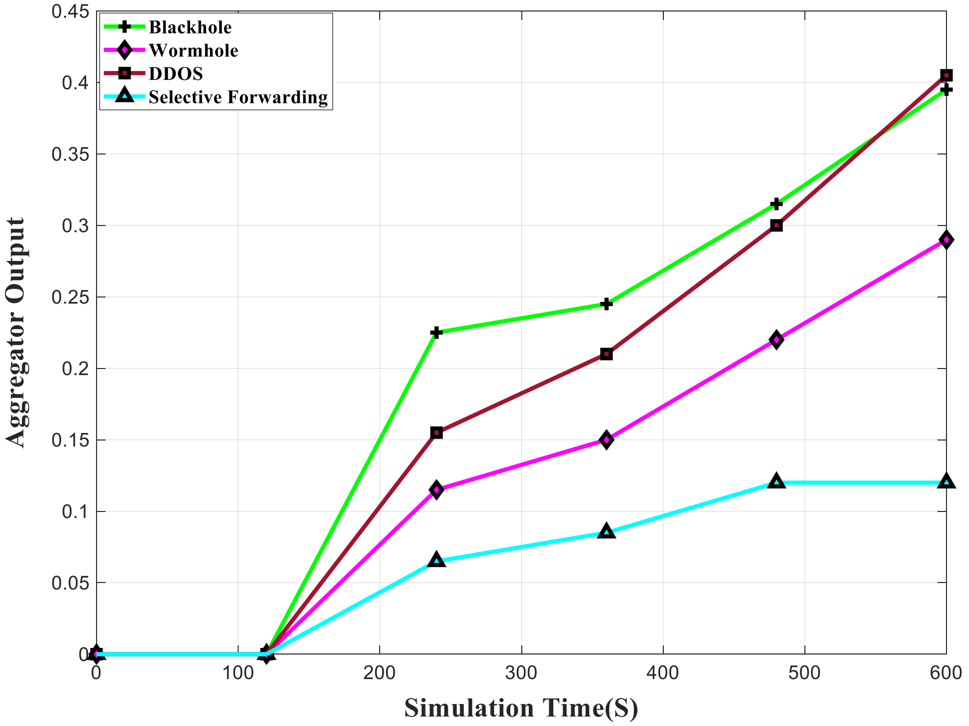


Figure 6.2 Aggregator Outputs

Iteration 2 gives the result of the second experiment, where the B-cell matches the anomalous peptides obtained from Iteration 1 and need not forward it to the Dendritic cell for further analysis, thereby conserving energy and memory. This is evident from Fig. 6.7 and Fig. 6.8. We can see a difference of Packet overhead when Iteration1 and Iteration 2 are compared.

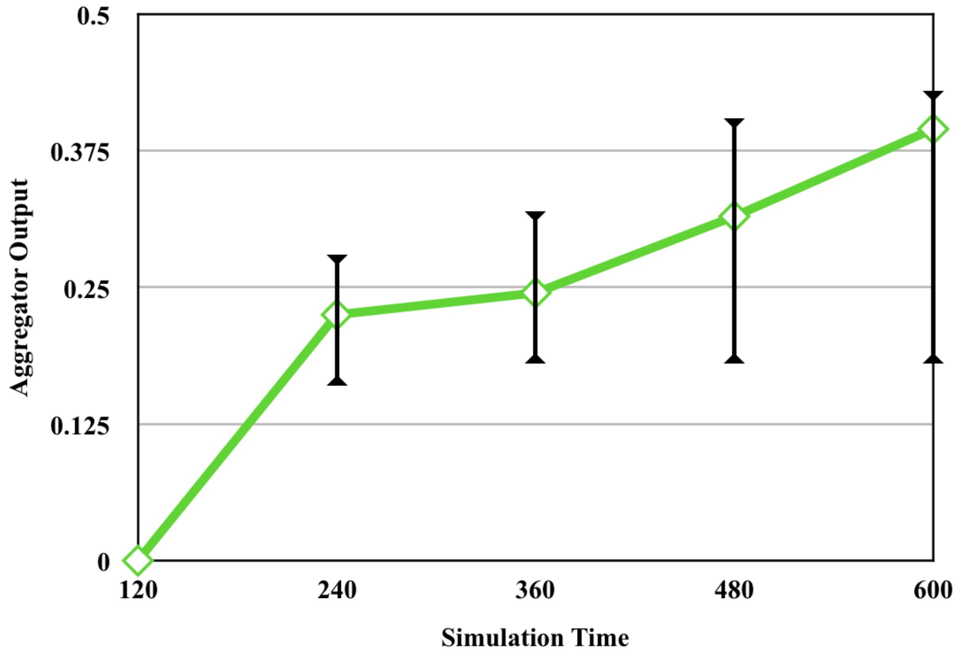


Figure 6.3 Aggregator Outputs for Blackhole Attack

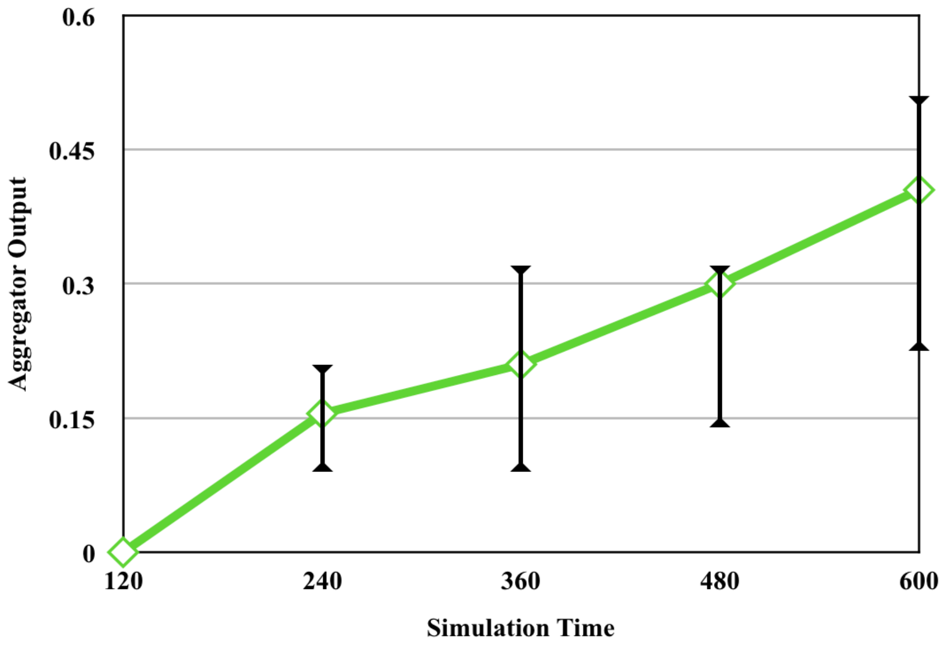


Figure 6.4 Aggregator Outputs for Flooding Attack

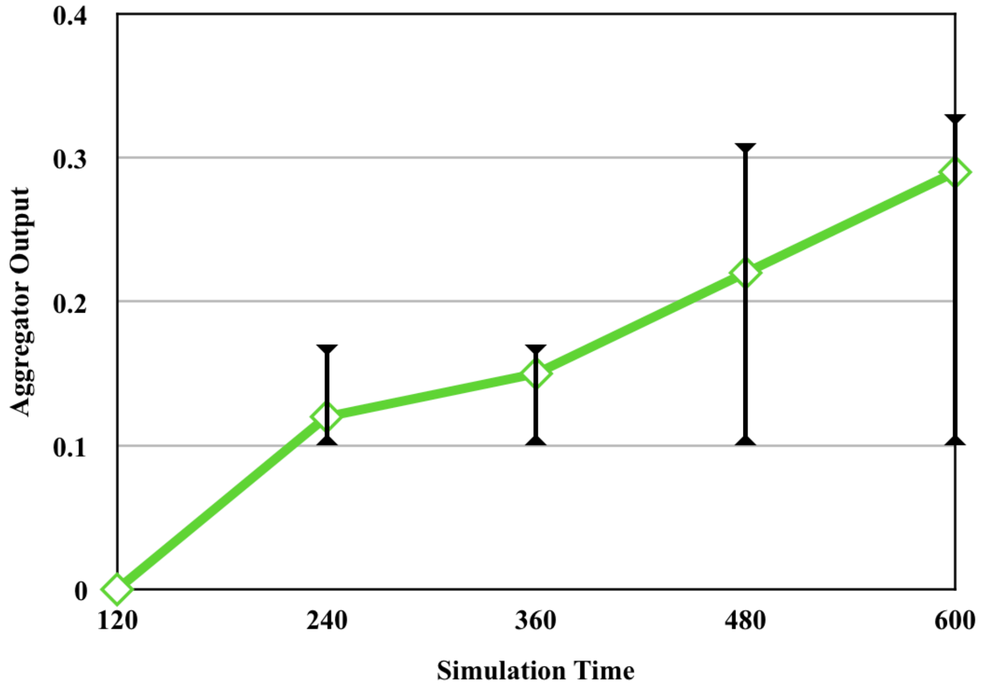


Figure 6.5 Aggregator Outputs for Wormhole Attack

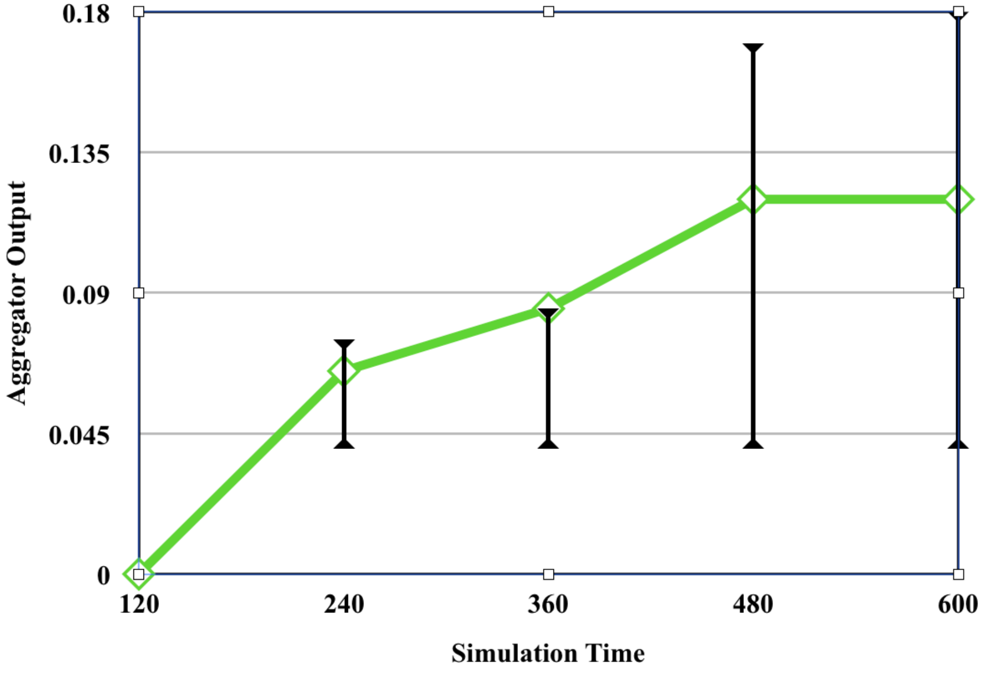


Figure 6.6 Aggregator Outputs for Selective Forwarding Attack.

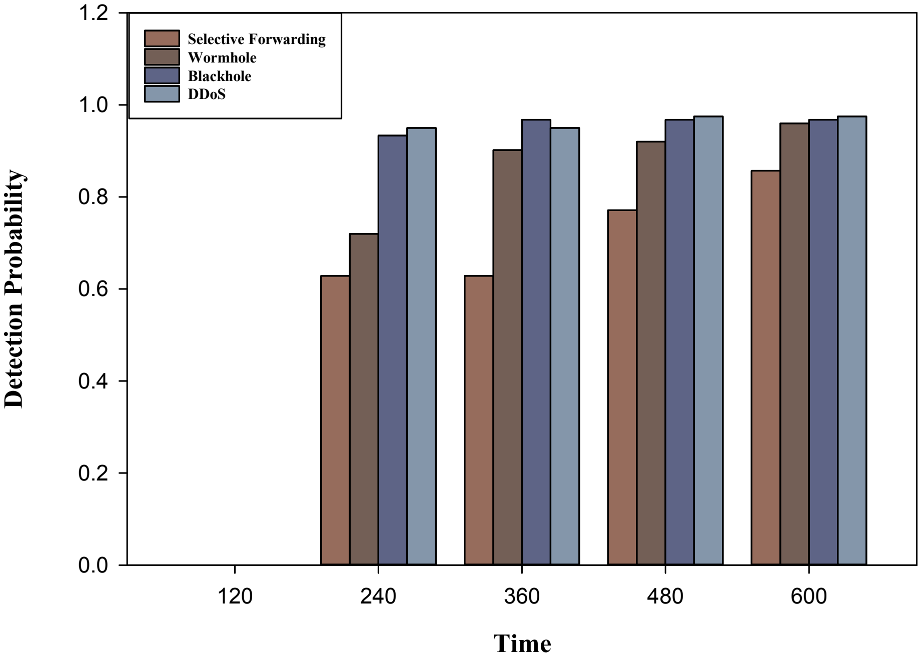


Figure 6.7 Probability of Detection of Each Attack.

This shows that the attack is detected early and the dendritic cell is not triggered. Fig. 6.8 shows that there is at least a 7% difference in the memory consumed by the IDS during Iteration1 and Iteration2. The total memory used by the IDS during iteration1 ranges from 9.2k,13.7k and 18.3k for nodes 20,30 and 40 respectively, which is significantly lower than the 48k ROM allocated in a sensor node. Since the B-memory stores strings of length 121 bits, a total of 3250 detector strings can be stored before the memory depletes. From Fig. 6.9, we can notice that there is a 14% increase in the energy dissipated when an IDS is in function for a 20-node network. This gets decreased to 8.3% during iteration2, indicating a difference of 5.7%. Similarly, the difference in energies from iteration1 and iteration2, for when the number of nodes is 30 and 40 are 7.5% and 7.7% respectively. This evidently proves that the difference in the energy dissipated is significant and the innate detection phase is efficient thereby saving a considerable amount of energy.

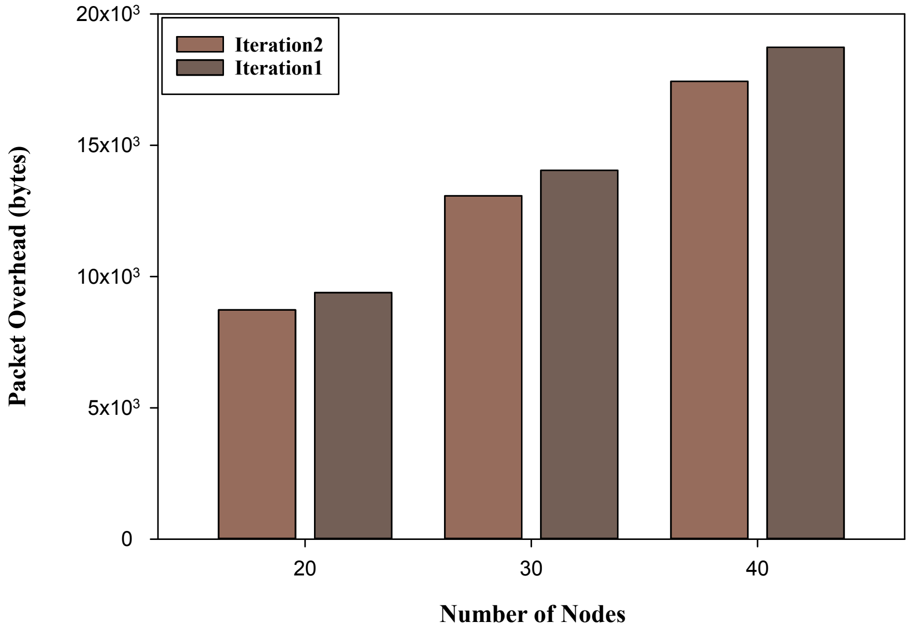


Figure 6.8 Packet Overhead Caused by the IDS

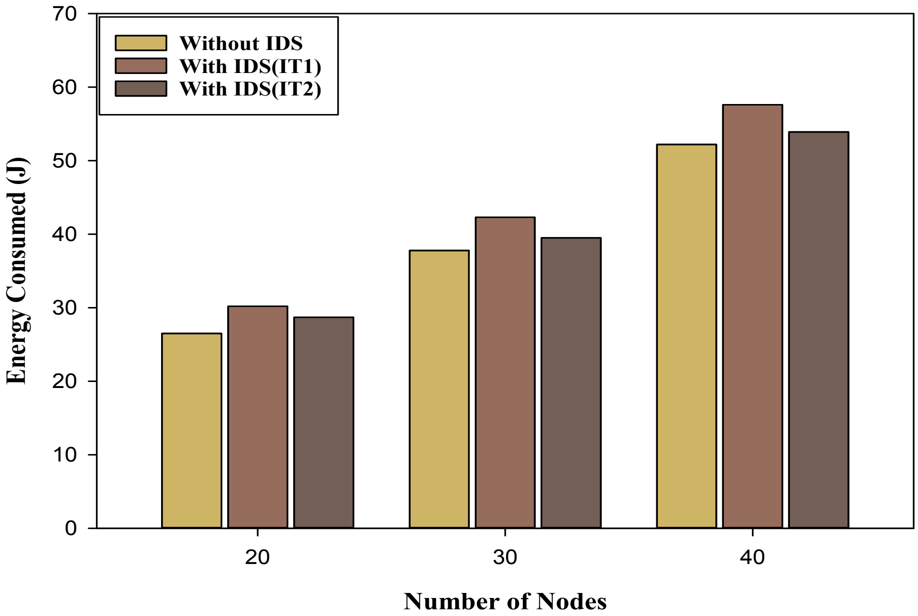


Figure 6.9 Energy Overhead Caused by the IDS

Table 6.1 Danger and PAMP Statistics

Attack	DS1				DS2				PS1				PS2				PS3				Aggregator Output
	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	T_1	T_2	T_3	T_4	
Blackhole (1)	10%	10%	10%	20%	20%	40%	60%	80%	20%	20%	40%	50%	0%	0%	0%	0%	60%	60%	60%	60%	0.395
Blackhole (2)	0%	10%	10%	10%	20%	40%	60%	60%	30%	30%	30%	30%	0%	0%	0%	0%	0%	40%	70%	70%	0.31
Blackhole (3)	10%	10%	10%	10%	20%	50%	50%	70%	10%	20%	20%	30%	0%	0%	0%	0%	20%	30%	50%	60%	0.30
Wormhole1	10%	20%	40%	60%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	2.21
Wormhole2	20%	30%	30%	50%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	40%	40%	40%	1.175
DDOS1(control packet flood)	30%	50%	60%	80%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	40%	40%	40%	40%	0.36
DDOS2(data flood)	10%	20%	40%	70%	20%	40%	60%	60%	0%	0%	0%	0%	20%	20%	20%	20%	40%	40%	40%	40%	0.405
Selective Forwarding 1	0%	0%	10%	10%	30%	30%	30%	40%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.075
Selective Forwarding 2	10%	10%	20%	20%	30%	50%	50%	50%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0.12

Below are a few comparisons for different attacks for danger theory-based algorithm.

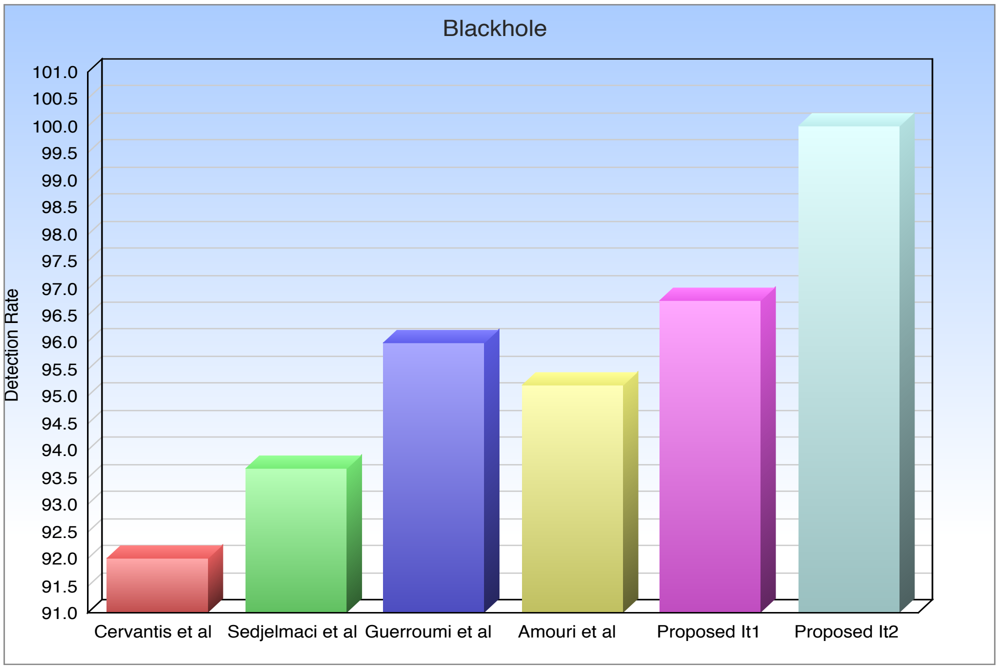


Figure 6.10 Comparisons of Different Algorithms for Blackhole Attack

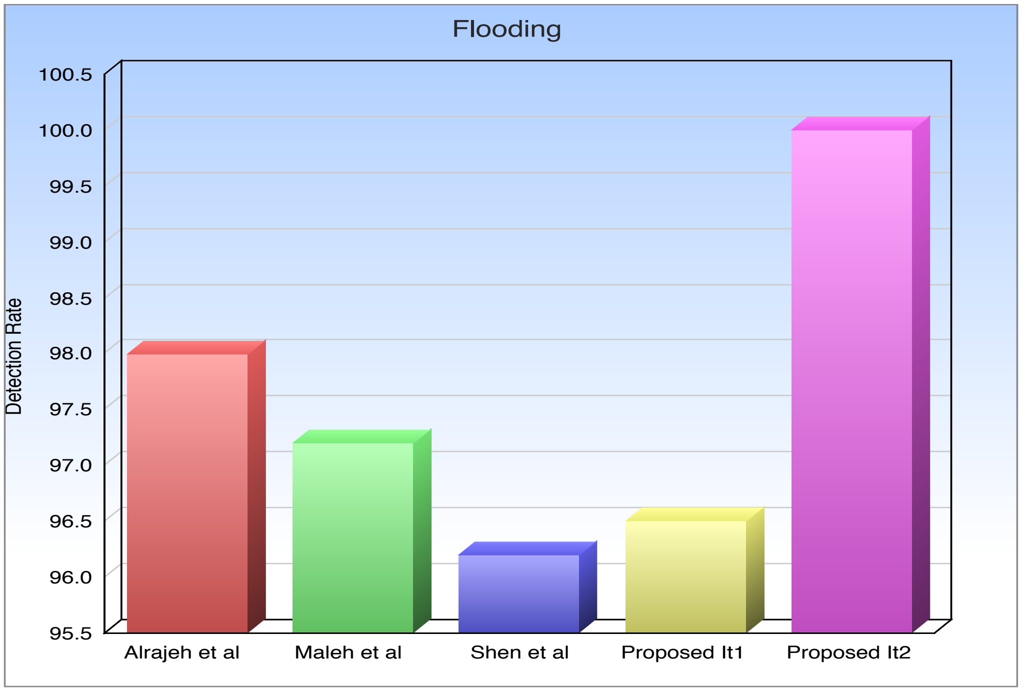


Figure 6.11 Comparisons of Different Algorithms for Flooding Attack

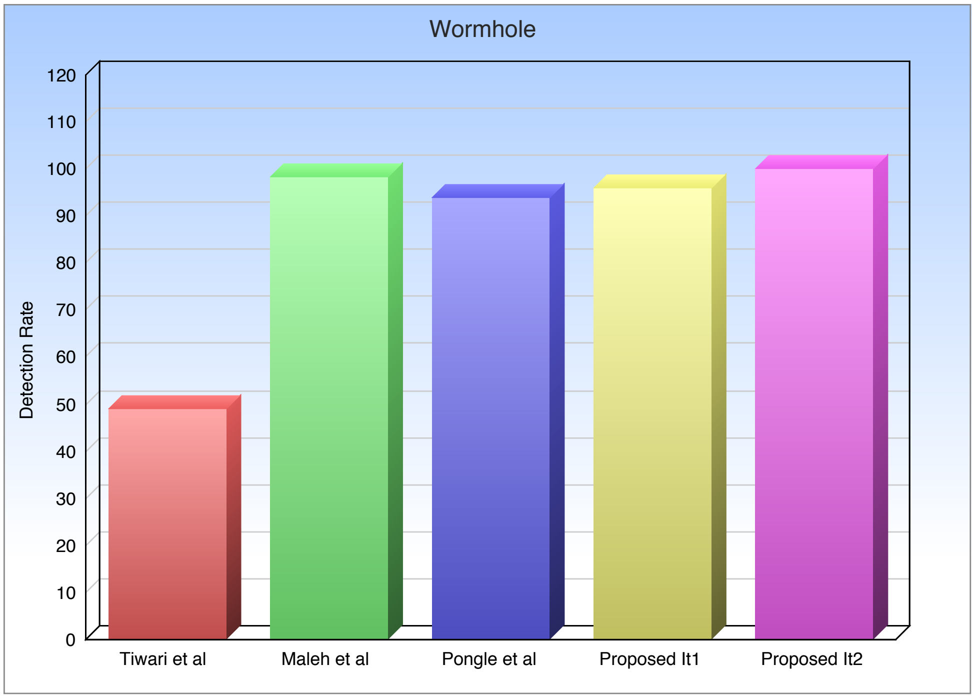


Figure 6.12 Comparisons of Different Algorithms for Wormhole Attack

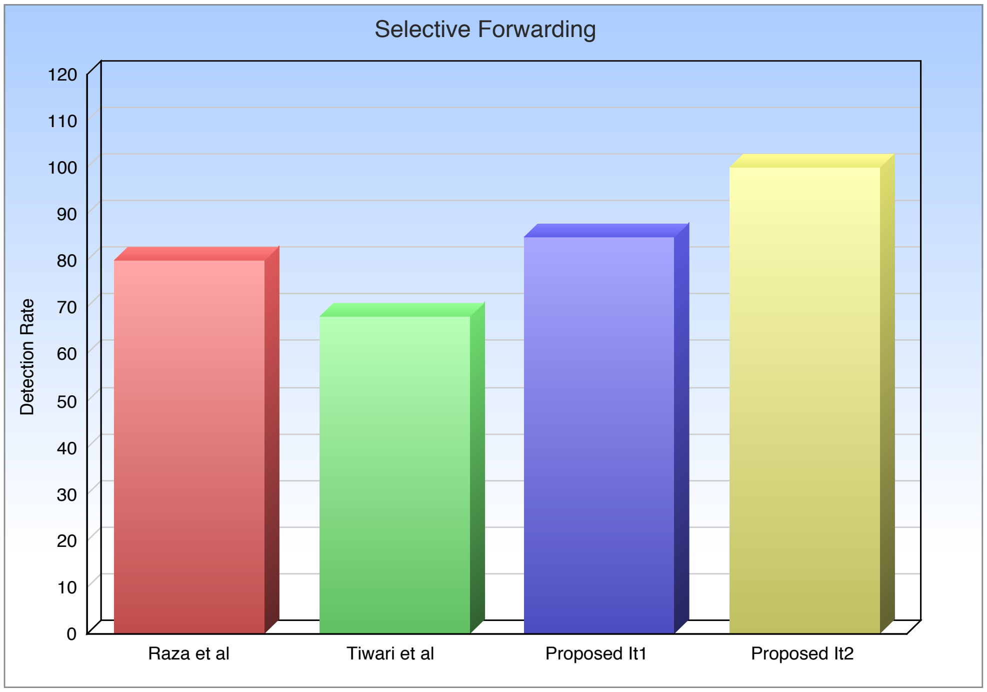


Figure 6.13 Comparisons of Different Algorithms for Selective Forwarding Attack

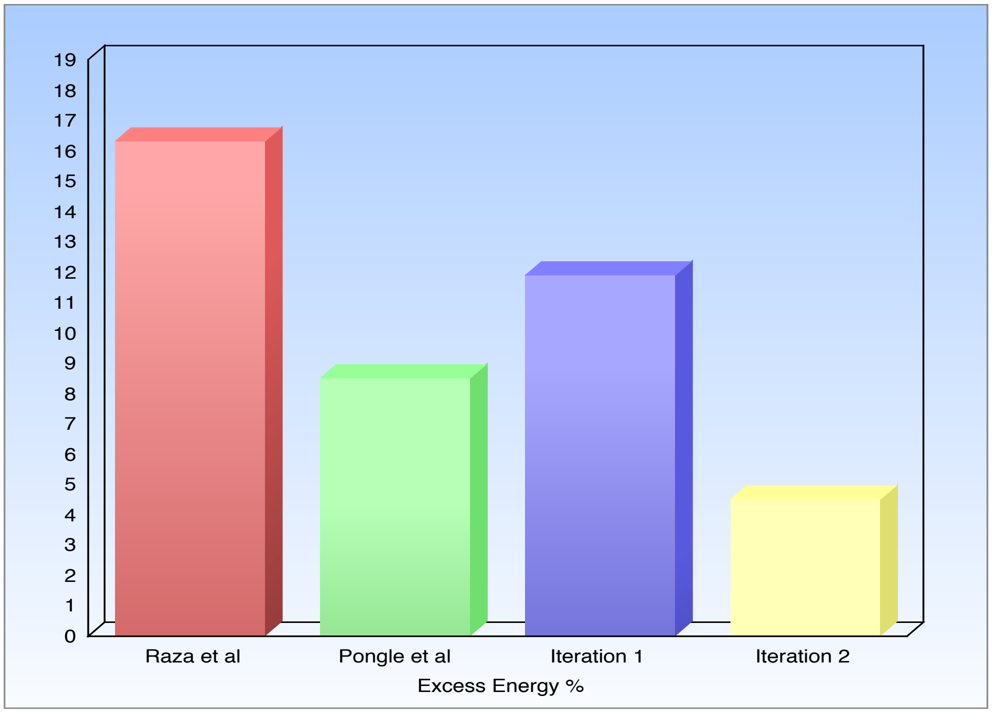


Figure 6.14 Comparisons of Different Algorithms for Energy Consumption

Fig 6.10 compares the performance of the proposed algorithm under a blackhole attack to the IDS in [86], [87], [88] and [54]. It should be noted that most IDS confine themselves to detecting a single attack. Hence, this work uses different works to compare for different attacks. The proposed system outperforms the mentioned algorithms by at least 0.6%.

Fig 6.11 compares the performance of the proposed algorithm under a flooding attack to the IDS in [89], [90] and [77]. Although most of the algorithms compared perform better than the proposed algorithm, our algorithm makes up for it during the second iteration.

Fig 6.12 compares the performance of the proposed algorithm under a wormhole attack to the IDS in [91], [90] and [92]. Only, Maleh et al has a slightly better detection rate than the proposed algorithm.

Fig 6.13 compares the performance of the proposed algorithm under a selective forwarding attack to the IDS in [93] and [91]. We can see that our IDS has a better detection rates than the rest of the works. For a more consistent comparison, it should be noted that [54], [92] and [93] use cooja as a simulator. Most of the other IDS's use NSL-KDD dataset.

Although this algorithm can detect a wide range of attacks with a very optimal energy and memory consumptions, the speed of detection is not quite optimal. However, a change can be noticed as the traffic density increases due to the aggregating nature of the proposed algorithm.

6.4.1.1 Schizophrenic Attacks

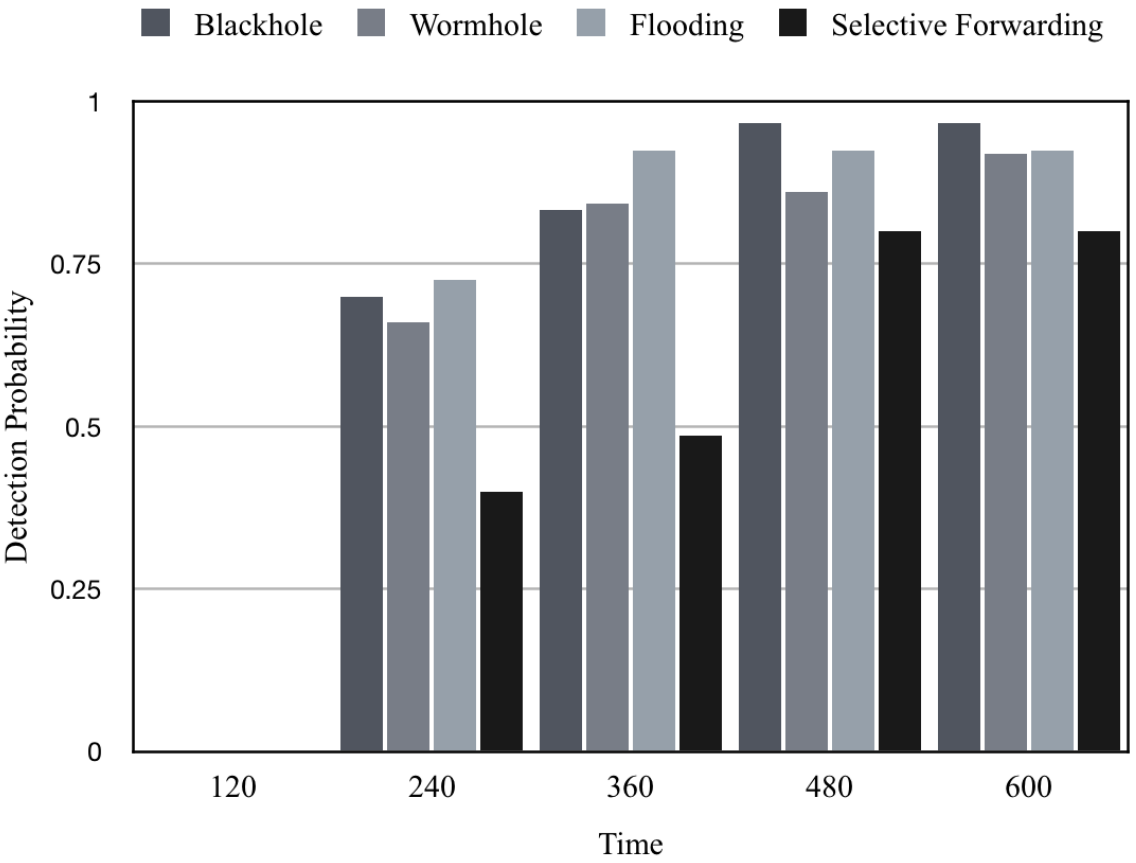


Figure 6.15 Probability of Detection of Schizophrenic Attacks

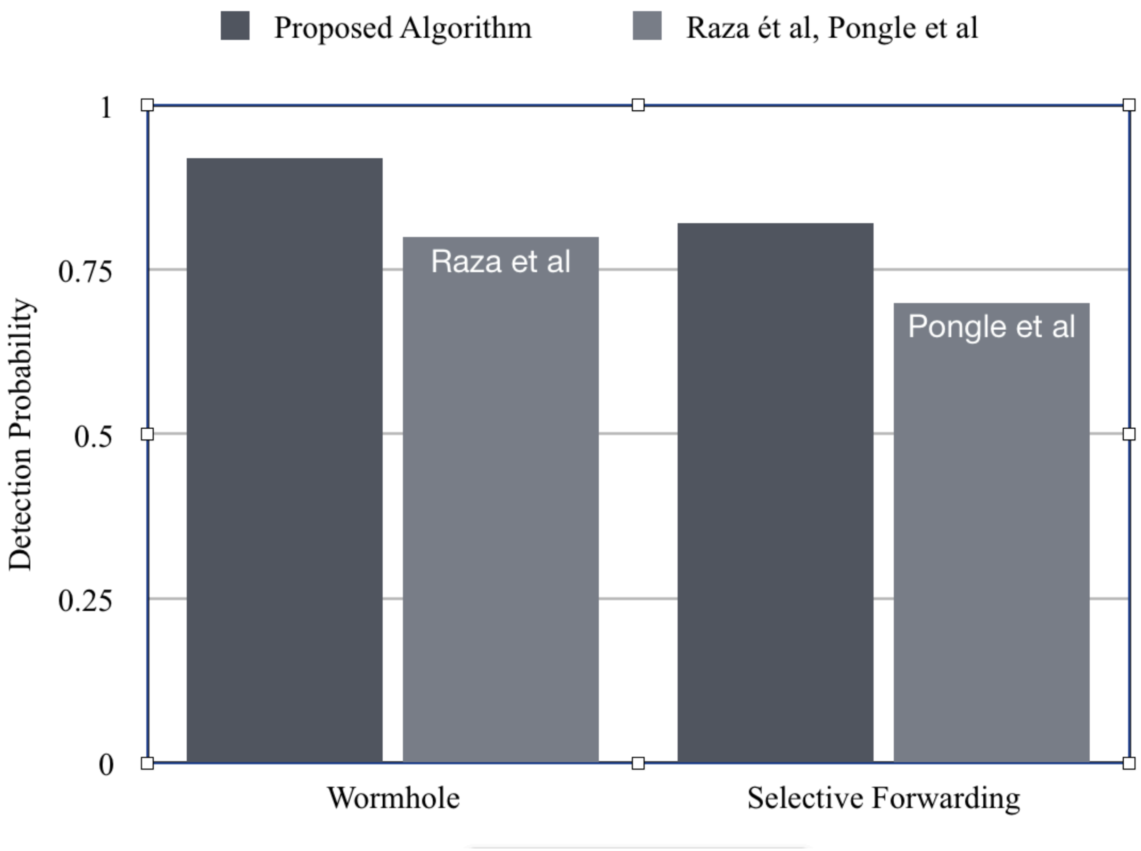


Figure 6.16 Comparisons of Different Algorithms for Schizophrenic Attacks.

Fig. 6.15 shows the resultant of an attacker in a 30-node network, the attack starting at 120 seconds. The attacks are time varying and follow a uniform distribution as mentioned in chapter 5. The aggregator output is calculated, and the detection is done at T_1=240s, T_2=360s, T_3=480s and T_4=600s for all the attacks mentioned earlier. The detection results follow a similar pattern to that of the network with malicious nodes, which has no time varying capabilities. However, there is a noticeable decrease in the rate of detection, when schizophrenic nodes are employed. This is due to the fact that the malicious nodes do not render enough malicious data to be aggregated as opposed to the non-time varying nodes, because the attacks do not occur for the entire functional time of the network. If the attack persists for a longer period, there will be a higher chance of detecting the attack.

Fig 6.16 gives a comparison of the IDS with other IDS's and it shows a considerable edge for the proposed IDS over the other two IDS's. Due to the limited amount of research done on IDS's for RPL protocol, this work is restricted to only two IDS's and two attacks to compare the proposed IDS against.

6.4.1.2 Classifying the Attacks

Table 6.2 gives a set of classification rules for the danger theory-based IDS. Although the proposed IDS can detect the attacks, it does not possess the ability to classify them. The set of rules presented in the table presents the necessary conditions which help to classify the attacks such as blackhole, flooding, wormhole and selective forwarding by using the concentrations of the danger and PAMP signals.

Table 6.2 Classification Rules

Classification Rule	**Attack**
If (C_{ds2} > 0.4 && C_{ds1} > 0.1 && C_{ps3} > 0.3)	***Blackhole***
If ((C_{ic1} ||C_{ic2}|| C_{ic3}) = 1 && C_{ds1} > 0.2)	***Wormhole***
If (C_{ds2} > 0.2 && C_{ds1} > 0.1 && C_{ps3} < 0.3)	***Selective Forwarding***
If (C_{ds2} = 0 && C_{ds1} > 0.3 && C_{ps3} > 0.3)	***Flooding***

6.4.2 Negative Selection

Fig 6.17 shows the detection rate and false positive rates of the algorithm when r = 69, 87 and 92 bits are contiguously matched and when the system is under a blackhole attack. r=69 indicates that only the first two features are used in the detection process. r=87 has another two features added to it. r=92 is the string with all the features embedded in it. As we can infer from the figure, the system has detection rates of 78.4, 86.2,86.2 and false positive rates of 7.8,5.8,5.8 for r= 69, 87 and 92 respectively. For better performance and based on the attacks, the order of the bit string can be changed to attain better detection rates for lower string values. The lesser the value of 'r' is, the lesser the number of features used in the detection process.

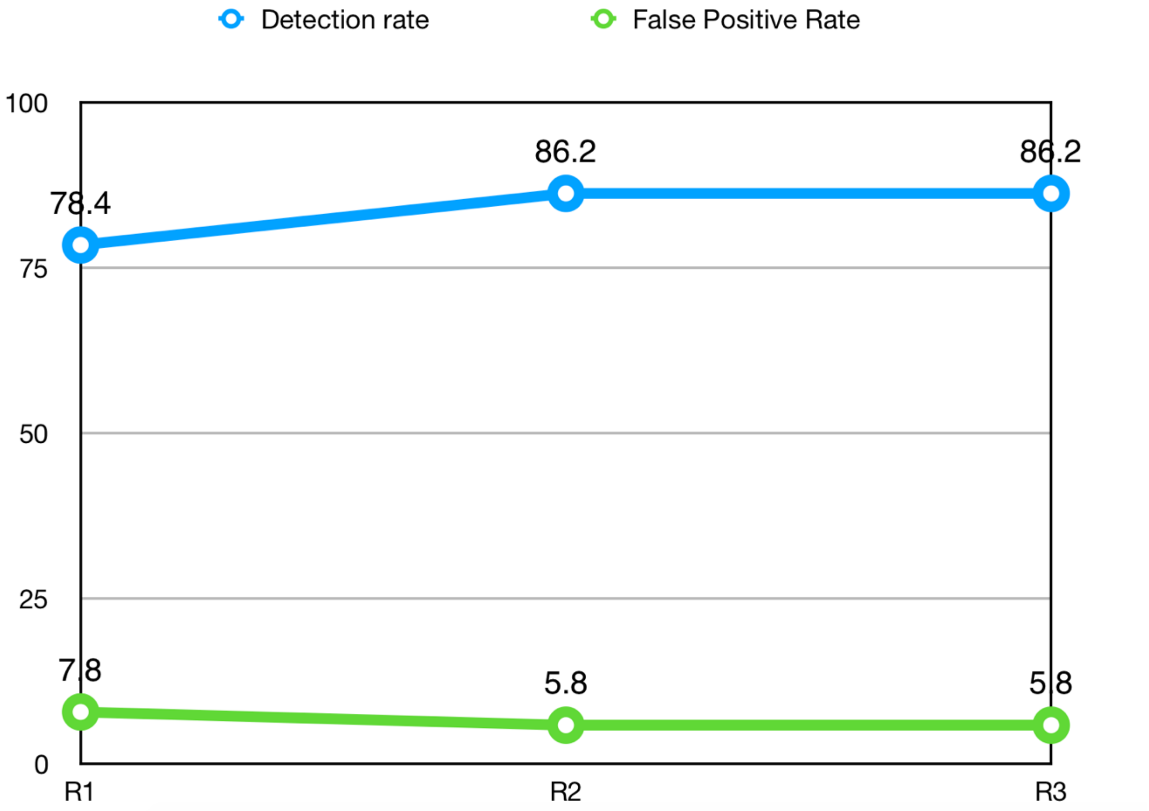


Figure 6.17 Detection and False Positive Rates of Blackhole Attack.

This translates to ‘the lesser the value of ‘r’ is, lower are the computational requirements and consequently, the energy required to process the IDS. However, the tradeoff is the number of true positives and false positives.

Fig 6.18 shows the detection rate and false positive rates of the algorithm when r = 69, 87 and 92 bits are contiguously matched and when the system is under a wormhole attack. As we can infer from the figure, the system has detection rates of 74.5, 78.4,88.2 and false positive rates of 3.9,3.9,1.9 for r= 69, 87 and 92 respectively. Wormhole attack has the lowest number of false positives.

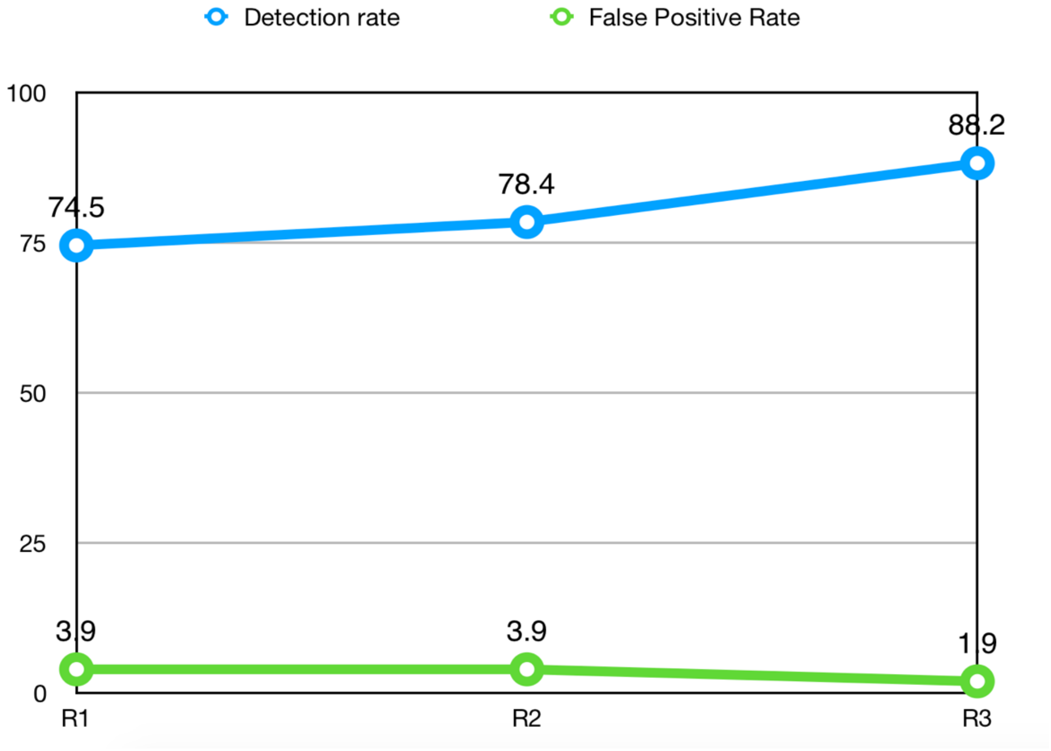


Figure 6.18 Detection and False Positive Rates of Wormhole Attack.

Fig 6.19 shows the detection rate and false positive rates of the algorithm when r = 69, 87 and 92 bits are contiguously matched and when the system is under a flooding attack. As we can infer from the figure, the system has detection rates of 82.3, 90.1,90.1 and false positive rates of 13.7,5.9,5.9 for r= 69, 87 and 92 respectively. Flooding attack has the best detection probability among other attacks. Fig 6.20 shows the detection rate and false positive rates for selective forwarding attacks. Selective forwarding attacks gives a significant number of false positives. However, the detection probability is as good as danger theory.

Although this algorithm can easily detect the attack profiles which are fed as antibodies during the training phase and has a perfect detection rate performing signature analysis, its performance is not quite optimal when unknown attack profiles are subjected to test during the testing phase. Although it still has a decent overall detection rate and provides faster execution and detection times, the major drawback is its functioning when a novel attack is implemented. To give an illustration of its performance, to achieve a 90% detection rate for blackhole or flooding attacks, the danger theory-based IDS needs at least 120 seconds. However, negative selection based AIS can do this almost instantly.

Therefore, this algorithm can easily be employed as signature analysis but not very preferable as an entirely anomaly-based system. To make the algorithm more robust, there is a need to produce more antibodies. This can be done by cloning or mutating the existing antibodies. However, as noted earlier, this cannot be done due to the regulated memory size in a WSN and the limited number of antibodies it can store.

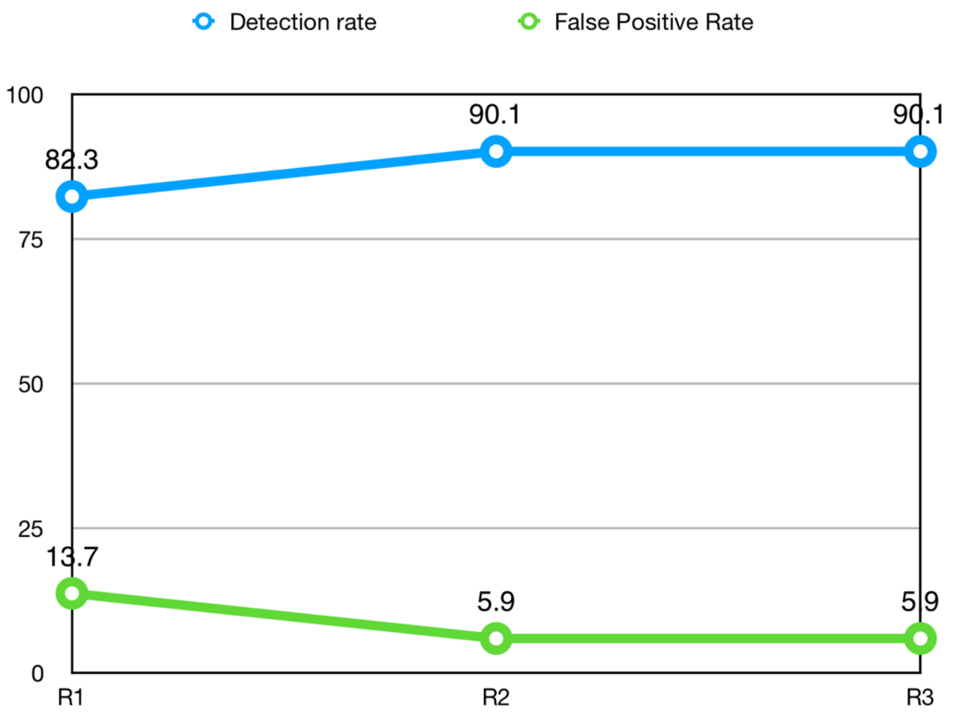


Figure 6.19 Detection and False Positive Rates of Flooding Attack.

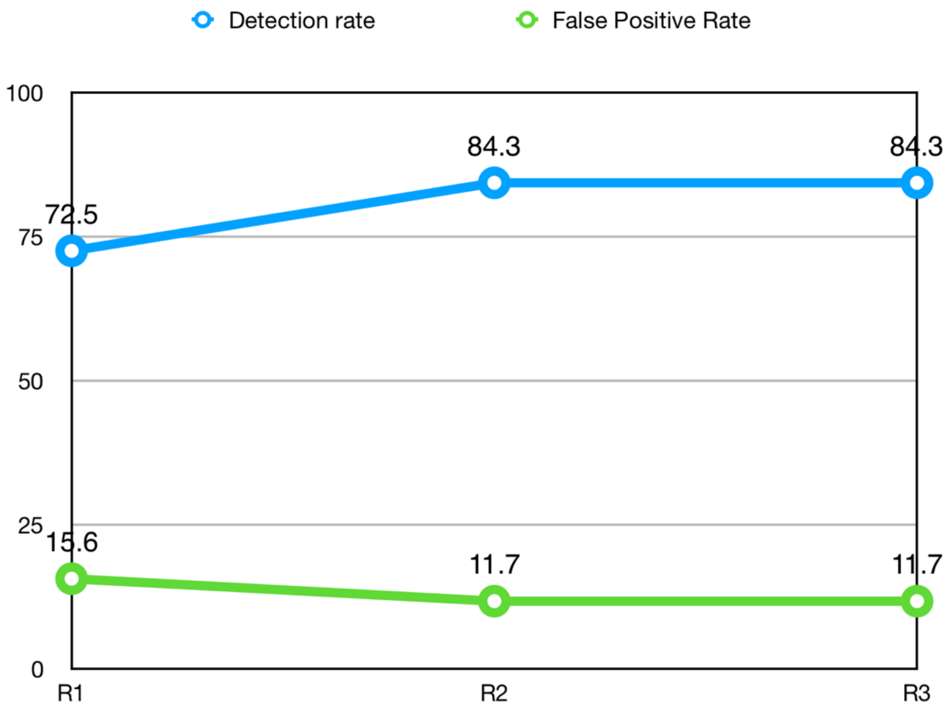


Figure 6.20 Detection and False Positive Rates of Selective Forwarding Attack.

CHAPTER 7: CONCLUSIONS AND FUTURE SCOPE

An IDS is designed by taking inspiration from the human immune system, while considering the resources that have the potential to affect the performance of a WSN. Although both these approaches are designed for WSNs, it can be easily modified for use on other resource constrained networks. Modifying the Danger signals generated through the dendritic node and the B-cell can help to adapt and extend this IDS to other networks including ADHOC networks. Although this model can predict different types of attacks, energy depleting attacks of any nature can be predicted more accurately and in a timely manner. It should be noted that any light weight signal generator which can find anomalies in the resource usage can be embedded into the skeleton of this model. Taking this into consideration, further studies will be done to make this model more robust and lightweight.

While trying to counter the aggressive attacking agents, the customary wireless sensor network poses a sizeable amount of problems such as lack of recognition, time lapse between detection and correction. Even when a danger theory-based IDS is employed, it requires a marginally higher than the optimal amount of time to detect an attack. The above-mentioned model based on negative selection tends to eliminate such problems. However, the negative selection-based IDS lack in the depth of detectability and produces considerable number of false positives. Further efforts are being made to implement the basophil and the T-cell nodes in order to build a more complete and robust system. That is, an Intrusion Mitigation System or a node correction mechanism is embedded into the existing system to make it a fully functional and automated system.

Finally, this area of research could see a massive growth through the support of additional immune aspects such as gene libraries and idiotypic networks. To conclude, research on the HIS is not comprehensive and there will be many more theories which will undoubtedly develop in time. As understanding of the HIS develops, the performance and capability of network IDS design based on this understanding will also improve.

REFERENCES

[1] Yick, J., Mukherjee, B. and Ghosal, D, “Wireless sensor network survey”, Computer networks, 52(12), pp.2292-2330,2008.

[2] Vieira, M.A.M., Coelho, C.N., Da Silva, D.C. and da Mata, J.M, Survey on wireless sensor network devices. In Emerging Technologies and Factory Automation. Proceedings. ETFA'03. IEEE Conference (Vol. 1, pp. 537-544),2003.

[3] Romer, K. and Mattern, F, The design space of wireless sensor networks. IEEE wireless communications, 11(6), pp.54-61,2004.

[4] Akyildiz, I.F. and Kasimoglu, I.H, Wireless sensor and actor☆ networks: research challenges. Ad hoc networks, 2(4), pp.351-367, 2004.

[5] Perrig,A., Stankovic, J. and Wagner, D,. Security in wireless sensor networks. Communications of the ACM, 47(6), pp.53-57,2004

[6] Dressler, F, Bio-inspired mechanisms for efficient and adaptive network security mechanisms. In Dagstuhl Seminar Proceedings. Schloss Dagstuhl-Leibniz-Zentrum für Informatik, 2005.

[7] Kim, J., Bentley, P.J., Aickelin, U., Greensmith, J., Tedesco, G. and Twycross, J, Immune system approaches to intrusion detection–a review. Natural computing, 6(4), pp.413-466, 2007.

[8] Hosseinpour, F., Bakar, K.A., Hardoroudi, A.H. and Kazazi, N., November. Survey on artificial immune system as a bio-inspired technique for anomaly based intrusion detection systems. In Intelligent Networking and Collaborative Systems (INCOS), 2010 2nd International Conference on (pp. 323-324). IEEE, 2010.

[9] Yin, C., Zhu, Y., Fei, J. and He, X, A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access, 5, pp.21954-21961,2017.

[10] Kolias, C., Kambourakis, G. and Maragoudakis, M, Swarm intelligence in intrusion detection: A survey. computers & security, 30(8), pp.625-642, 2011.

[11] Dorigo, M. and Stützle, T, Ant colony optimization: overview and recent advances. In Handbook of metaheuristics pp. 311-351). Springer, Cham,2019.

[12] W. Hao, Z. Yuqing, "AraTRM: Attack Resistible Ant-based Trust and Reputation Model", Proc. IEEE Int'l. Conf. Computer and Information Technology, pp. 652-57, 2014

[13] R. V. Kulkarni, G. K. Venayagamoorthy, "Neural Network based Secure Media Access Control Protocol for Wireless Sensor Networks", Proc. IEEE Int'l Joint Conf. Neural Networks, pp. 1680-87, 2009.

[14] Bitam, S., Zeadally, S. and Mellouk, A, Bio-inspired cybersecurity for wireless sensor networks. IEEE Communications Magazine, 54(6), pp.68-74,2016.

[15] E. W. Fulp, "An Evolutionary Strategy for Resilient Cyber Defense", Proc. IEEE Globecom, pp. 1-6, 2015.

[16] Li, D., Liu, S. and Zhang, H, Negative selection algorithm with constant detectors for anomaly detection. Applied Soft Computing, 36, pp.618-632,2015

[17] Alaparthy, V.T. and Morgera, S.D, A Multi-Level Intrusion Detection System for Wireless Sensor Networks Based on Immune Theory. IEEE Access, 6, pp.47364-47373,2018.

[18] De Castro, L.N. and Von Zuben, F.J, July. The clonal selection algorithm with engineering applications. In Proceedings of GECCO ,Vol. 2000, pp. 36-39),2000.

[19] Alaparthy, V.T., Amouri, A and Morgera, S.D, A study on the Adaptability of Immune models for Wireless Sensor Network Security, proceedings of biologically inspired cognitive architectures in procedia Computer Science,Elsevier, to be published (2018)

[20] F. Hosseinpour, P. V. Amoli, F. Farahnakian, J. Plosila and T. Hämäläinen, "Artificial Immune System Based Intrusion Detection: Innate Immunity using an Unsupervised Learning Approach," International Journal of Digital Content Technology and its Applications, vol. 8, no. 5, October 2014.

[21] J. Greensmith, U. Aickelin and S. Cayzer, "Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection," in Proceedings of the 4th International Conference on Artificial Immune Systems, Banff.

[22] K.-m. kim, H. Kim and K. Kim, "Design of an Intrusion Detection System for Unknown-attacks based on Bio-inspired Algorithms," in Computer Security Symposium 2015, 2015.

[23] S. Forrest, A. S. Perelson, L. Allen and R. Cherukuri, "Self-Nonself Discrimination in a Computer," in proceedings of the 1994 IEEE Symposium on Security and Privacy.

[24] J. Vidal, A. Orozco and L. J. G. Villalba, "Adaptive artificial immune networks for mitigating DoS flooding attacks," Swarm and Evolutionary Computation, pp. 94-108, July 2017.

[25] W. Lou, W. Liu, Y. Fang, SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks, IEEE INFOCOM 2004, 2004.

[26] Acharya, R., Asha, K. (2008, December). Data integrity and intrusion detection in wireless sensor networks. In Networks, 2008. ICON 2008.

[27] Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, G. J. (2000). Protocols for self-organization of a wireless sensor network. IEEE personal communications, 7(5), 16-27

[28] Pathan, A. S. K., Lee, H. W., Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE

[29] Lee, J. C., Leung, V. C., Wong, K. H., Cao, J., Chan, H. C. (2007). Key management issues in wireless sensor networks: current proposals and future developments. IEEE Wireless Communications, 14(5).

[30] Becher, A., Benenson, Z., Dornseif, M. (2006, April). Tampering with motes: Real-world physical attacks on wireless sensor networks. In International Conference on Security in Pervasive Computing (pp. 104-118). Springer, Berlin, Heidelberg.

[31] Modares, H., Salleh, R., Moravejosharieh, An Overview of security issues in wireless sensor networks. In Computational Intelligence, Modelling and Simulation (CIMSiM), 2011 Third International Conference on (pp. 308-311). IEEE, 2011.

[32] Newsome, J.; Shi, E.; Song, D.; Perrig, A. The sybil attack in sensor networks: Analysis and defences.In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, Berkeley, CA, USA, 2627 April 2004.

[33] F. Anjum and P. Mouchtaris, Security for Wireless Ad Hoc Networks, Wiley-Interscience, New York, NY, USA, 1st edition, 2007.

[34] Win, K. S., Analysis of detecting wormhole attack in wireless networks. In World Academy of Science, Engineering and Technology,2008.

[35] Ramaswamy, S. Prevention of Cooperative Blackhole Attack in Wireless Ad-hoc Networks. Int. Conf. Wirel. Netw.2003.

[36] Srinivas, V.B.; Umar, S. Spoofing Attacks in wireless Sensor Networks. IJCSET 2013, 3, 201210.

[37] Dubey, A.; Meena, D.; Gaur, S. A Survey in Hello Flood Attack in Wireless Sensor Networks. Int. J. Eng. Res. Technol.2014, 3.

[38] Zhang, Y.; Minier, M. Selective Forwarding Attacks against Data and ACK Flows in Network Coding and Countermeasures. J. Comput. Netw. Commun. 2012, 2012, 184783

[39] Luo, X., Ji, X., Park, M. S. (2010, April). Location privacy against traffic analysis attacks in wireless sensor networks. In Information Science and Applications (ICISA), 2010 International Conference on (pp. 1-6). IEEE.

[40] Virmani, D., Soni, A., Chandel, S., Hemrajani, M. (2014). Routing attacks in wireless sensor networks: A survey. arXiv preprint arXiv:1407.3987.

[41] Abdullah, M.Y.; Hua, G.W.; Alsharabi, N. Wireless sensor networks misdirection attacker challenges and solutions. In Proceedings of the International Conference on Information and Automation, Changsha, China, 2023 June 2008; pp. 369373.

[42] Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V. Denial of service attacks in wireless networks: The case of jammers. IEEE Commun. Surv. Tutor. 2011, 13, 245257.

[43] Reindl, P.; Nygard, K.; Du, X. Defending malicious collision attacks in wireless sensor networks. In Proceedings of the IEEE/IFIP Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, China, 1113 December 2010.

[44] Ding, J. Defending against path-based DoS attacks in Wireless Sensor. In Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 05), New York, NY, USA, 7 November 2005; pp. 8996.

[45] Shaukat, H.R.; Hashim, F.; Sali, A.; Rasid, M.F.A. Node Replication Attacks in Mobile Wireless Sensor Network: A Survey. Int. J. Distrib. Sens. Netw. 2014, 2014, 115.

[46] Abawajy, J. H. (Ed.). (2012). Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications: Theoretical Frameworks and Practical Applications. IGI Global.

[47] Flammini, F. (2012). Critical infrastructure security: assessment, prevention, detection, response. WIT Press.

[48] Diaz, A., Sanchez, P. (2016). Simulation of attacks for security in wireless sensor network. Sensors, 16(11), 1932.

[49] Singh, V.P.; Jain, S.; Singhai, J. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. Int. J. Comput. Sci. Issues 2010, 7, 2327.

[50] Zhou, L.; Wu, D.; Zheng, B.; Guizani, M. Joint physical-application layer security for wireless multimedia delivery. IEEE Commun. Mag. 2014, 52, 6672.

[51] Abdelkarim, A.A. and Nasereddin, H.H, Intrusion prevention system. International Journal of Academic Research, 3(1), p.201,2011.

[52] Butun, I., Morgera, S.D. and Sankar, R, A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), pp.266-282,2014.

[53] Amouri, A., Morgera, S.D., Bencherif, M.A. and Manthena, R, A Cross-Layer, Anomaly-Based IDS for WSN and MANET. Sensors, 18(2), p.651,2018.

[54] Amouri, A., Alaparthy, V.T. and Morgera, S.D, Cross layer-based intrusion detection based on network behavior for IoT in Wireless and Microwave Technology Conference (WAMICON), 2018 IEEE 19th (pp. 1-4). IEEE,2018.

[55] Mishra, A., Gupta, B.B. and Joshi, R.C, A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques. In Intelligence and Security Informatics Conference (EISIC), 2011 European(pp. 286-289). IEEE.,2011.

[56] Herbert, T.B. and Cohen, S., 1993. Stress and immunity in humans: a meta-analytic review. Psychosomatic medicine, 55(4), pp.364-379.

[57] V. T. Alaparthy, S. Morgera, "Modelling an intrusion detection system based on adaptive immunology", Int. J. Interdiscipl. Telecommun. Netw..,to be published, 2019.

[58] P. Matzinger, "The Danger Model: A Renewed Sense of Self," Science, vol. 296, no. 5566, pp. 301-305.

[59] Parthasarathy, K. (2014). Clonal selection method for immunity based intrusion, detection systems. Project Report, 1-19.

[60] Robert L. Fanelli, A Hybrid Model for Immune Inspired Network Intrusion Detection Springer journal, pp. 107118,2008.

[61] Dasgupta, D. (2006). Advances in artificial immune systems. IEEE computational intelligence magazine, 1(4), 40-49.

[62] J. Timmis, M. Neal, and J. Hunt, An Artificial Immune System for Data Analysis, In the Proceedings of the International Workshop on Intelligent Processing in Cells and Tissues (IPCAT), 1999.

[63] Xiao, R.B., Wang, L. and Liu, Y, A framework of AIS based pattern classification and matching for engineering creative design. In Machine Learning and Cybernetics, 2002. Proceedings. 2002 International Conference on (Vol. 3, pp. 1554-1558). IEEE,2002.

[64] Kim, J., Wilson, W.O., Aickelin, U. and McLeod, J, August. Cooperative automated worm response and detection immune algorithm (cardinal) inspired by t-cell immunity and tolerance. In International Conference on Artificial Immune Systems (pp. 168-181). Springer, Berlin, Heidelberg,2005.

[65] Knight, T. and Timmis, J, A multi-layered immune inspired machine learning algorithm. In Applications and Science in Soft Computing (pp. 195-202). Springer, Berlin, Heidelberg,2004.

[66] Shamshirband, S., Anuar, N. B., Kiah, M. L. M., Rohani, V. A., Petkovi, D., Misra, S., Khan, A. N,. Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks. Journal of Network and Computer Applications, 42, 102,117. review. Psychosomatic medicine, 55(4), pp.364-379,2014.

[67] Aickelin,U., Cayzer.,S, The danger theory and its application to Artificial Immune systems.arXiv preprint arXiv:0801.3549,2008.

[68] Greensmith, J., Aickelin, U. and Cayzer, S. : Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Intrusion Detection, In Proc. of ICARIS-05, SpringerVerlag (2005) 153-167

[69] Kim, J., Bentley, P., Wallenta, C., Ahmed, M., Hailes, S. (2006). Danger is ubiquitous: Detecting malicious activities in sensor networks using the dendritic cell algorithm. Artificial Immune Systems, 390-403

[70] Sarafijanovic, S. and Le Boudec, J. : An AIS for misbehaviour detection in mobile ad-hoc networks with virtual thymus, clustering, danger signals and memory detectors, In Proc. of the 2rd Int. Conf. on AIS (ICARIS-04), Springer-Verlag (2005) 342-356

[71] Rizwan, R., Khan, F. A., Abbas, H., Chauhdary, S. H, Anomaly detection in Wireless Sensor Networks using immune-based bioinspired mechanism. International journal of distributed sensor networks, 11(10), 684952, 2015.

[72] Hofmeyr, S., Forrest, S., Architecture for an artificial immune system, Evolutionary Computation, 2000, 8(4): 443473.

[73] Hofmeyr, S., (1999) An Immunological Model of Distributed Detection and Its Application to Computer Security, PhD Thesis, Dept of Computer Science, University of New Mexico, 1999.

[74] J. Percus, 0. Percus, and A. Perelson. Predicting the size of the antibody combining region from consideration of efficient self/non-self discrimination. Proc. of the National Academy of Science, 90:1691-1695, 1993

[75] J. Gomez, F. Gonz alez, and D. Dasgupta, An immuno-fuzzy approach to anomaly detection, in Proceedings of the 12th IEEE International Conference on Fuzzy Systems (FUZZ 03), pp. 1219 1224, Baton Rouge, La, USA, May 2003.

[76] Kim, J. and Bentley, P. J. (2002), Immune Memory in the Dynamic Clonal Selection Algorithm. , Proceedings of the First International Conference on Artificial Immune Systems (ICARIS) Canterbury, pp.5765, September 9-11, 2002.

[77] W. Shen, G. Han, L. Shu, J. Rodrigues and N. Chilamkurthi, "A New Energy Prediction Approach for Intrusion Detection in Cluster-Based Wireless Sensor Networks," in International Conference on Green Communications and Networking, Berlin, 2011

[78] C. Vasar, O. Prostean, I. Filip, R. Robu and D. Popescu, "Markov models for wireless sensor network reliability," in IEEE 5th International Conference on Intelligent Computer Communication and Processing, 2009.

[79] Suliman, S.I., Shukor, M.S.A., Kassim, M., Mohamad, R. and Shahbudin, S,.Network Intrusion Detection System Using Artificial Immune System (AIS). In 2018 3rd International Conference on Computer and Communication Systems (ICCCS) (pp. 178-182). IEEE,April 2018.

[80] Ji, Z. and Dasgupta, D, V-detector: An efficient negative selection algorithm with "probably adequate" detector coverage. Information sciences, 179(10), pp.1390-1406,2009.

[81] M. Zeeshan, H. Javed and S. Ullah, "Discrete R-Contiguos Bit Matching Mechanism Appropriateness for Anomaly Detection in Wireless Sensor Networks," International Journal of Communication Networks and Information Security, vol. 9, no. 2, August 2017.

[82] WANG, Y. and FANG, K, A note on uniform distribution and experimental design. In Selected Papers Of Wang Yuan(pp. 417-421),(2005)

[83] Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J.P. and Alexander, R., 2012. RPL: IPv6 routing protocol for low-power and lossy networks(No. RFC 6550).

[84] Eriksson, J., Österlind, F., Finne, N., Tsiftes, N., Dunkels, A., Voigt, T., Sauter, R. and Marrón, P.J.,. COOJA/MSPSim: interoperability testing for wireless sensor networks. In Proceedings of the 2nd International Conference on Simulation Tools and Techniques (p. 27). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009.

[85] Mulligan, G, The 6LoWPAN architecture. In Proceedings of the 4th workshop on Embedded networked sensors (pp. 78-82). ACM,2007.

[86] Cervantes, C., Poplade, D., Nogueira, M., & Santos, A, Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things. In Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on (pp. 606-611). IEEE,2015.

[87] Sedjelmaci, H., & Feham, M, Novel hybrid intrusion detection system for clustered wireless sensor network. arXiv preprint arXiv:1108.2656, 2011

[88] Guerroumi, M., Derhab, A., & Saleem, K, Intrusion detection system against sink hole attack in wireless sensor networks with mobile sink. In Information Technology-New Generations (ITNG), 2015 12th International Conference on (pp. 307-313). IEEE,2015.

[89] Alrajeh, N. A., Khan, S., Mauri, J. L., & Loo, J, Artificial Neural Network Based Detection of Energy Exhaustion Attacks in Wireless Sensor Networks Capable of Energy Harvesting. Ad Hoc & Sensor Wireless Networks, 22(1-2), 109-133,2014.

[90] Maleh, Y., Ezzati, A., Qasmaoui, Y., & Mbida, M, A global hybrid intrusion detection system for wireless sensor networks. Procedia Computer Science, 52, 1047-1052,2015

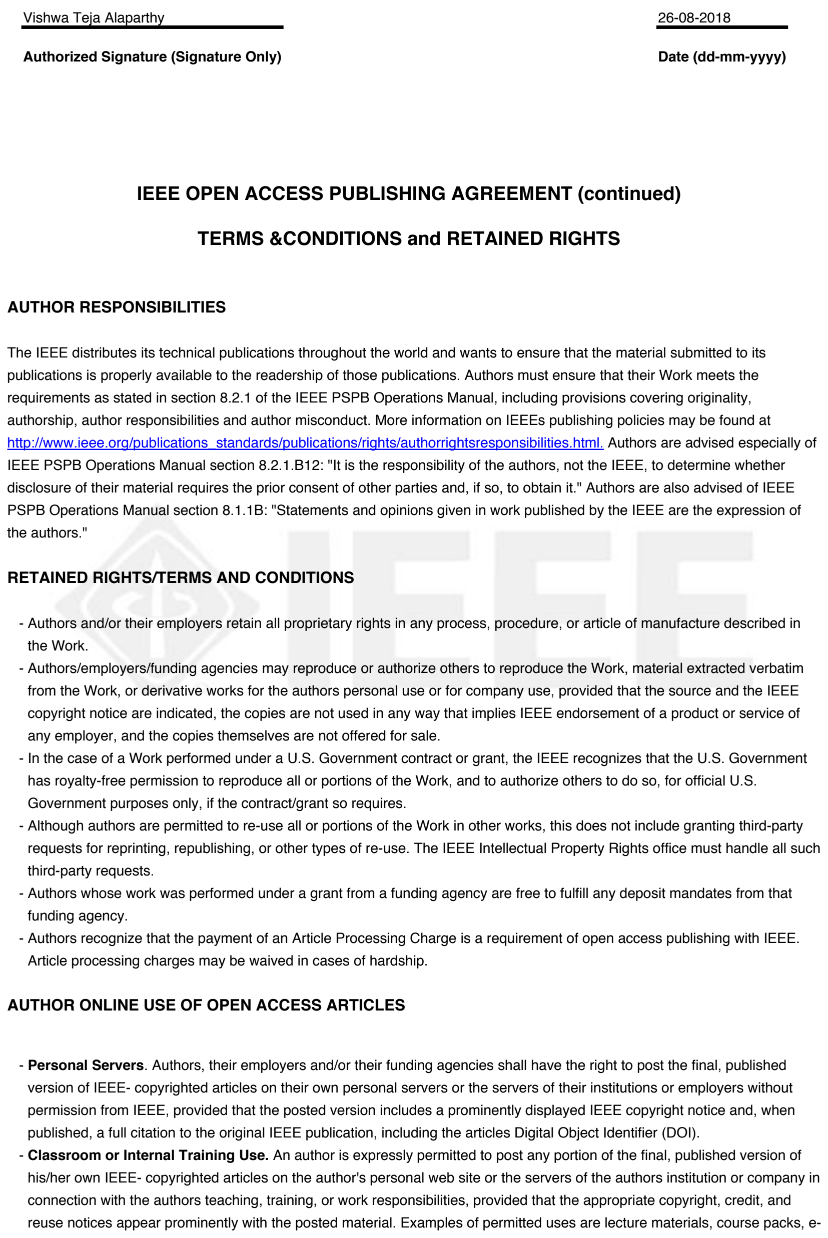
[91] Tiwari, M., Arya, K. V., Choudhari, R., & Choudhary, K. S, Designing intrusion detection to detect black hole and selective forwarding attack in wsn based on local information. In Computer Sciences and Convergence Information Technology, 2009. ICCIT'09. Fourth International Conference on (pp. 824-828). IEEE,2009.

[92] Pongle, P., & Chavan, G, Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications, 121(9),2015.

[93] Raza, S., Wallgren, L., & Voigt, T, SVELTE: Real-time intrusion detection in the Internet of Things. Ad hoc networks, 11(8), 2661-2674,2013

APPENDIX A: COPYRIGHT PERMISSIONS

The permission below is for the use of material in chapter 5 and parts of chapter 3 and 6.



Vishwa Teja Alaparthy

Authorized Signature (Signature Only)

26-08-2018

Date (dd-mm-yyyy)

IEEE OPEN ACCESS PUBLISHING AGREEMENT (continued)

TERMS &CONDITIONS and RETAINED RIGHTS

AUTHOR RESPONSIBILITIES

The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEEs publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html. Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

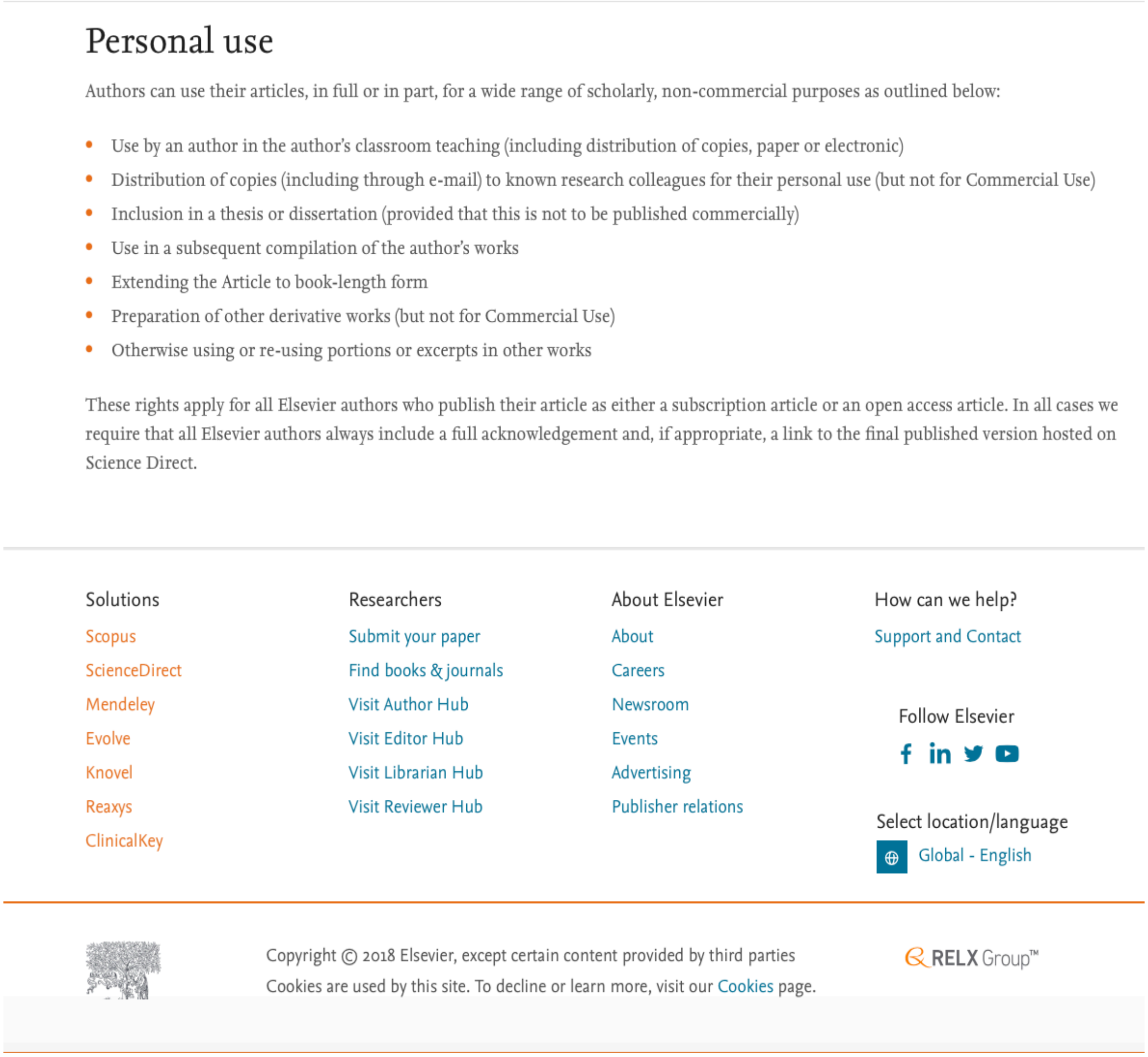
RETAINED RIGHTS/TERMS AND CONDITIONS

- Authors and/or their employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
- Authors/employers/funding agencies may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the authors personal use or for company use, provided that the source and the IEEE copyright notice are indicated, the copies are not used in any way that implies IEEE endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
- In the case of a Work performed under a U.S. Government contract or grant, the IEEE recognizes that the U.S. Government has royalty-free permission to reproduce all or portions of the Work, and to authorize others to do so, for official U.S. Government purposes only, if the contract/grant so requires.
- Although authors are permitted to re-use all or portions of the Work in other works, this does not include granting third-party requests for reprinting, republishing, or other types of re-use. The IEEE Intellectual Property Rights office must handle all such third-party requests.
- Authors whose work was performed under a grant from a funding agency are free to fulfill any deposit mandates from that funding agency.
- Authors recognize that the payment of an Article Processing Charge is a requirement of open access publishing with IEEE. Article processing charges may be waived in cases of hardship.

AUTHOR ONLINE USE OF OPEN ACCESS ARTICLES

- **Personal Servers**. Authors, their employers and/or their funding agencies shall have the right to post the final, published version of IEEE- copyrighted articles on their own personal servers or the servers of their institutions or employers without permission from IEEE, provided that the posted version includes a prominently displayed IEEE copyright notice and, when published, a full citation to the original IEEE publication, including the articles Digital Object Identifier (DOI).
- **Classroom or Internal Training Use.** An author is expressly permitted to post any portion of the final, published version of his/her own IEEE- copyrighted articles on the author's personal web site or the servers of the authors institution or company in connection with the authors teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-

The permission below is for the use of material in chapter 4.



Personal use

Authors can use their articles, in full or in part, for a wide range of scholarly, non-commercial purposes as outlined below:

- Use by an author in the author's classroom teaching (including distribution of copies, paper or electronic)
- Distribution of copies (including through e-mail) to known research colleagues for their personal use (but not for Commercial Use)
- Inclusion in a thesis or dissertation (provided that this is not to be published commercially)
- Use in a subsequent compilation of the author's works
- Extending the Article to book-length form
- Preparation of other derivative works (but not for Commercial Use)
- Otherwise using or re-using portions or excerpts in other works

These rights apply for all Elsevier authors who publish their article as either a subscription article or an open access article. In all cases we require that all Elsevier authors always include a full acknowledgement and, if appropriate, a link to the final published version hosted on Science Direct.