Summer 2010

Distributed spatiotemporal detection for chemical and biological threats using human immune mechanisms

Yatin Bodas

Department:

DISTRIBUTED SPATIOTEMPORAL DETECTION FOR CHEMICAL AND BIOLOGICAL THREATS USING HUMAN IMMUNE MECHANISMS

by

YATIN BODAS

A THESIS

Presented to the Faculty of the Graduate School of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

2010

Approved by

Sanjeev Agarwal, Advisor
Jagannathan Sarangapani
Hai Xiao

ABSTRACT

Ubiquitous detection of chemical and biological (CB) threats in an urban environment using widely distributed, low-cost, broad-spectrum sensors carried by public or on vehicles is extremely desirable and pertinent for homeland security. These distributed sensors should interoperate autonomously and adaptively to meet stringent operational and detection performance requirements. This research explores the use of scalable detection methodology, inspired by the human immune mechanisms to meet these challenges. An adaptive spatiotemporal control mechanism is proposed to organize the detection behavior of spatially dispersed sensors using peer-to-peer communication so that a shorter response time, higher probability of detection and lower false alarm rates (FARs) are achieved at the system level even though individual sensors have only modest performance capabilities. The detection mechanism is developed to minimize the power consumption and required density of the detectors while achieving the desired performance requirements. Different tradeoffs between deployment strategies for the sensors and system level performance requirements are discussed. The effectiveness of the algorithm is demonstrated by carrying out extensive scaled simulations using agent-based models. Based on these simulation studies, some recommendations on the individual sensor performance requirements and achievable system level objectives are presented.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my Advisor, Dr. Sanjeev Agarwal, for providing me incessant support and guidance throughout this research. I would also like to express my gratitude towards Dr. Jagannathan Sarangapani and Dr. Hai Xiao for giving their valuable time in reviewing my work and for being on my committee. I would also like to thank Shivakar Vulli and Dheeraj Singiresu for helping me in my research. Both of them have helped me at different stages in this research. I would also like to gratefully acknowledge the financial support from Leonard Wood Institute (LWI) and Intelligent Systems Center (ISC) at Missouri University of Science and Technology. Finally I would like to thank my parents for their constant motivation which helped me complete my research and studies.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1. INTRODUCTION

Chemical and biological (CB) agents coupled with improvised explosive devices (IEDs) not only present a great danger to soldiers and civilian lives, but are also extremely difficult to detect and neutralize in an urban setting [1]. Many contact/exposure based techniques for detecting CB-threats, including gas/liquid chromatography, mass/ion mobility spectrometry [2,3] have been well studied. Standoff detection techniques including Raman spectroscopy and laser induced breakdown spectroscopy [4–8] have also been studied more recently. Over the recent years, several electro-optical techniques, including infrared spectrometry [9], terahertz sensing [10] hyperspectral imaging [11] and fluorescence characterization [12] for detecting CB-threats have also been presented. Efforts to develop an electro-chemical sensor based detection platform have also been reported [13]. Since all of these sensors are limited in detection range, ubiquitous detection requires the use of many such sensors dispersed over a wide area. In order to be used practically, these sensors should meet the stringent performance requirements and should be inexpensive enough to be used in large numbers. The requirement of inexpensive sensors leads to them having modest performance capabilities. Here, a scalable detection methodology, inspired by the human immune mechanisms is presented to meet the required performance requirements even in the presence of these limitations for individual sensors.

The human immune system (HIS) is known to effectively tackle similar challenges. For example, an infection occurring in the body is detected in a relatively small time with minimal allergic reactions (false alarms). Taking motivation from these highly effective human immune mechanisms, an adaptive spatiotemporal control

mechanism is presented to organize the detection behavior of spatially dispersed sensors using peer-to-peer communication so that a shorter response time, higher probability of detection and lower FARs are achieved at the system level. The detection mechanism is developed to minimize the power consumption and required density of the sensors while achieving desired performance requirements similar to the human immune system where detection of an infection occurs without hampering other bodily functions. Different tradeoffs between deployment strategies for the sensors and system level performance requirements are discussed. Since verification of these strategies using real world experiments is difficult, the effectiveness of the algorithm is demonstrated by carrying out extensive scaled simulations. The outcomes of experiments where large number of agents interact with each other are inherently complex to study and model. Agent based modeling techniques are found to be suitable for studying such scenarios [32]. Thus simulations have been developed as agent based models. Based on these simulation studies, some recommendations on the individual sensor performance requirements and achievable system level objectives are presented.

The remainder of the thesis is outlined as follows. Chapter 2 describes the problem statement. Chapter 3 discusses about the mechanisms of the human immune system relevant in this research. Chapter 4 explains the experimental setup and the simulation system and the various software packages used for this research. Chapter 5 contains the relevant analytical models and shows their comparisons with the simulation results. Chapter 6 talks about the two techniques developed to assist the mechanisms of the HIS. The results obtained from the simulated experiments are discussed in Chapter 7.

The conclusions derived from these results are discussed in Chapter 8 with some comments on possible future work and future investigation of the approach.

2. PROBLEM STATEMENT

With an increase in the security threat posed by terrorists through IEDs combined with CB-threats of various types, it is highly desirable to develop sensors which are capable of detecting them over a wide area. Moreover, to have the capability of detection in a wide area, deploying large number of sensors for wide variety of possible threats can be challenging. In such scenarios, having sensors which are low in cost and which consume less power are extremely desirable for practical use. Having low cost sensor design can possibly result in sensors having large FARs. Getting multiple detections i.e. reconfirmations from distinct sensors can result in less FARs at system level but this in turn increases the time-to-detection as additional time is taken for each reconfirmation. Having sensors capable of detecting threats from a wide range can result in higher power consumption and/or an increase in the time-to- detection. There is a need to develop a detection methodology with which a system has all the features of wide-band detection, less power consumption, small detection time and less FARs. Different tradeoffs need to be negotiated while the achievable sensor performance needs to be determined.

In scenarios where there is a call to detect CB-threats which could be placed anywhere in large areas, the detection time can be kept small only if there are a large number of detectors spread throughout the field. Miscreants can easily target different parts of large urban areas by placing IEDs coupled with CB-threats in them. The usual techniques of detecting such threats like using sniffer dogs or sophisticated equipments are only useful for smaller areas where they can be moved around in lesser time. But these techniques are impractical for detection in large areas as the time required to move

around a single piece of equipment would naturally take large amount of time and energy of the personnel handling them. A feasible solution to this is to have large number of detectors spread throughout the area. Moreover when such detectors are mounted on public vehicles which move around throughout the area, they can provide round the clock surveillance for possible threats resulting in true ubiquitous detection, which is essential to homeland security.

It is extremely desirable to keep the cost of the detectors small. While deploying detectors in large quantities, higher cost of individual detectors can result in extremely large procurement costs, making such a solution impractical. Low cost detectors can result in sensors having less sensitivity and specificity. This can happen due to many reasons. To make the detectors low in cost, the lower cost components may have high tolerances resulting in less performance in terms of sensitivity and specificity. Also some shortcomings in the sensing materials may not be addressed as better materials generally result in higher costs. The drawback of having detectors with less sensitivity can be mitigated by having more number of detectors. If the specificity of detectors is lower (i.e. the false alarm rate is high) increasing the number of detectors can further increase the combined number of false alarms resulting from them. An intelligent mechanism needs to be developed to suppress these FARs at the system level.

In order to have detectors capable of sensing multiple types of CB-threats, corresponding number of sensor probes have to be mounted in them, each capable of sensing threats from a limited band of threats. Each probe would have a biasing circuit associated with it. More number of probes would result in more number of circuits and each circuit needs to be supplied with power. Thus an increase in the types of threats that

the detector can sense results in more power consumed by it. Ideally such detectors mounted on public vehicles should not require frequent battery changes. A technique needs to be developed which when used with the system gives wide band detection capability while having detectors that consume minimal power. One possibility explored here is to lower the power consumption by time scheduling the detectors, so that only one type of threat is detected at a given time. The resulting performance tradeoffs are discussed.

To summarize the problem statement, wide area detection requires a large number of detectors which necessitate the use of low cost detectors. These low cost detectors result in high FARs. Wide band detection results in more sensor probes and biasing circuits and with that an increase in the power consumption. A detection technique needs to be developed which provides all the desirable features of low cost, low FARs, high detection probability, wideband detection, small detection time and low power consumption.

In this research various mechanisms of the human immune system have been studied and relevant mechanisms were applied for detection of CB-threats that may occur anywhere in a wide area. Lower system-level FARs are achieved even in the case when individual sensor have high FARs and lower probability of detection. The detection time is minimized while the detection probability is maximized for a given set of parameters. Techniques are developed which minimized the power consumption of the sensors even in the case of them having capability of sensing threats from a wide spectrum. Different tradeoffs between deployment strategies for the sensors and the system level performance requirements are discussed. Different agent based modeling software packages were

studied and an appropriate package was selected. Simulations were then developed using agent based modeling techniques. The effectiveness of the algorithm is demonstrated by running these simulations and gathering and analyzing the data collected from them. Based on these simulation studies, some recommendations on the individual sensor performance requirements and achievable system level objectives are presented.

3. HUMAN IMMUNE SYSTEM

The human immune system is a highly complex system of interacting cells and molecules responsible for identifying and engaging harmful non-self agents. The immune system as a whole has the capabilities to recognize and eliminate a myriad of foreign agents (approximately 10^{11}) [33] , distinguish them from noninfectious self cells and molecules, and statistically remembering each detected foreign agent to ensure efficient handling of a second exposure to the agent. The immune system can be broadly divided into the innate immune system and adaptive immune system. While innate immune system represents the ability to recognize and destroy certain foreign agents, inherent from birth, the adaptive immune system represents the ability to identify and deal with pathogens encountered during the life of the organism [15,16]. Of the numerous mechanisms employed by the human immune system, few, including clonal selection, secondary immune response and negative selection, have received considerable attention from the Artificial Immune Systems (AIS) community [17,18].

3.1. CLONAL SELECTION

Pattern recognition is most basic task of the immune system. The immune system should recognize and eliminate all harmful foreign agents that enter the body. In practice the HIS is capable of recognizing and eliminating most types of foreign agents. Lymphocytes (B and T cells) are mainly responsible for pattern recognition. Each lymphocyte has about 10^4 to 10^5 receptors [33] on its surface which are all of the same type. Lymphocytes detect an antigen when a molecular bond is established between the antigen and the receptors on its surface. In order to detect diverse types of antigens, the immune system maintains a variety of the receptors in the body. Thus in an event of an

antigen entering the body, whether any lymphocyte is able to detect that antigen can be viewed as a random event. But once a cell recognizes the antigen it quickly forms clones of itself and thus more such cells are introduced in the system. This ensures that there are enough antibodies in the system capable of detecting and eliminating similar type of antigens to prevent an infection and improve the time-to-detection. This process is called clonal selection because only those types of cells proliferate (clone) which are able to recognize the antigen that the body is exposed to, while other cells maintain their normal densities.

3.2. SECONDARY IMMUNE RESPONSE- LEARNING AND MEMORY

The number of lymphocytes having a particular type of receptor is limited. For example, a mouse contains about 10^8 lymphocytes in its body. If it maintains 10^7 types of receptors, then it has only 10 lymphocytes of any particular type present at any given time. Thus there are only a small number of lymphocytes present in the body which are able to identify any particular antigen. As a result, the probability of detecting an antigen is small, increasing the time-to-detection. The immune system has an intrinsic reinforced learning mechanism by which, once an antigen is successfully recognized, subsequent encounters with the antigen produces a faster response. This is accomplished using memory cells which are produced during the clonal selection process. Low quantities of these memory cells remain in dormant state until activated by a repeated exposure to an antigen [19]. Figure 3.1 shows the primary and secondary responses in the immune system. After the antigen-A is dealt with a primary response, subsequent encounter with antigen-A produces a rapid and stronger response, even in the presence of another antigen-B.

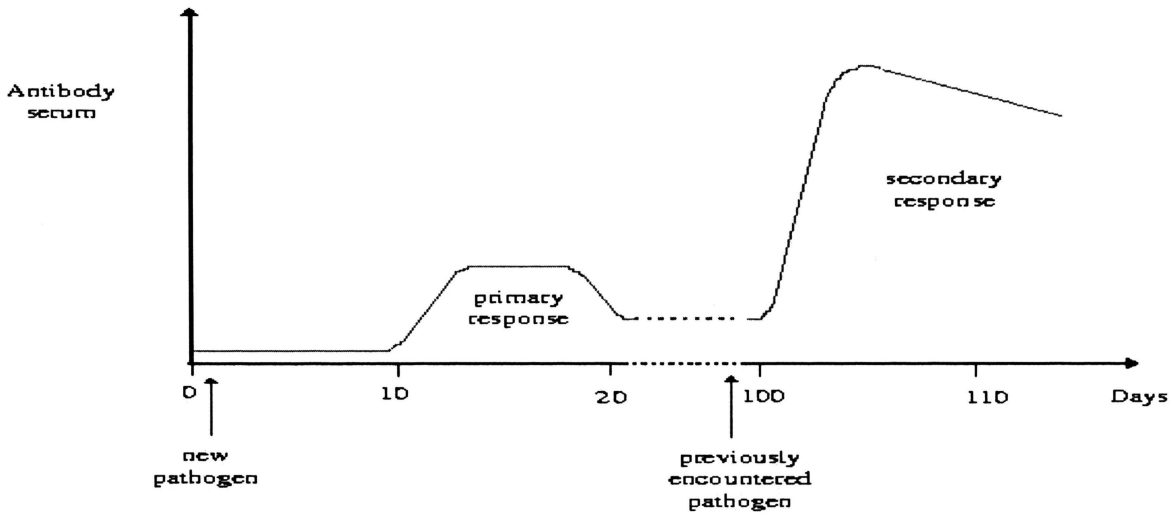

Figure 3.1. Primary and Secondary Responses

3.3. APPLICATIONS OF HIS

Algorithms inspired by the mechanisms of the immune system have been implemented in a variety of fields. Clonal selection has been used for optimization [20,21] and classification [22]. Negative selection based algorithms have been extensively studied for intrusion and anomaly detection [23–26]. Algorithms derived from learning in immune systems have been used in the fields of robotics [27] and clustering [28]. Detailed surveys on applications of AIS in a variety of fields can be found in De Castro and Zuben (1999, 2000) [17,18], Dasgupta et al. (2003) [29] and Hart(2009) [30].

3.4. APPLICATION OF HIS MECHANISMS IN DETECTION OF THREATS

The immune mechanisms of clonal selection, secondary response, learning and memory can be applied to achieve shorter response time, low power consumption and low FARs while having the capability of broad spectrum detection. These mechanisms

are particularly useful in the scenario when detectors are fitted with small sensor probes, each one capable of sensing CB-threats from a limited spectrum and each one having a dedicated biasing circuit associated with it which can be independently switched ON/OFF and where the detectors are interconnected with each other with the help of a wireless network. Interconnectivity between sensors either via peer-to-peer routing or via a central communication tower [14] is desired as it enables information to be shared among the sensors and to gather intelligence to a central station. Instead of supplying power to all the circuits at all times, each circuit is supplied power for only a small period of time (time-slice) and exactly one circuit is supplied with power at any given time. Figure 3.2 shows one possible sequence of the time division multiplexing (TDM) scheme in which the sensors can be turned ON and OFF.

threat : 1	threat : 2	threat : 3	.....	threat : g-2	threat : g-1	threat : g

Figure 3.2. One Possible Sequence of Switching the Sensor Circuits

By this method, power is virtually supplied only to a single circuit at any given time instead of all the circuits, thus saving on power. The time-slices in which the sensor probes are turned ON can be thought of as lymphocytes. Because of the TDM scheme, a variety of receptors are maintained in the system.

3.4.1. Application of the Clonal Selection Mechanism. While moving in the field, if a detector comes in a patch of area where a particular type of threat is present, it can only sense it if the corresponding circuit present inside it is powered ON at that time.

In normal conditions, detectors allocate equal number of time-slices to all the sensor circuits. So if the detector has 'g' number of sensor circuits, the probability that a particular circuit is on (or it senses the threat present near it) is 1/g. This probability can be increased if the detector is somehow provided the knowledge of the type of threat present in its vicinity and it allocates more time-slices to that type. This can be achieved in the following way. Once any detector (with a probability of 1/g) senses a threat in its vicinity, it can share this information about the type of the threat with other detectors which are within a certain distance from it using the communication network. Upon reception of this information, all the detectors can increase the number of time-slices allotted for sensing the reported type of threat. Thus, even though the first detection is made with the probability of 1/g, it is possible to get subsequent detections (i.e. reconfirmations) from nearby detectors with an increased probability. If these surrounding detectors now allocate 'n' time slices, the threat can be detected with a probability of n/g. A shorter response time is thus achieved because of this increase in probability of detection. By increasing the time-slices for only the reported type of threat, the clonal selection mechanism of the HIS is emulated in which the population of only those cells which detected the antigen is increased.

In more detail, the algorithm for the clonal selection mechanism would be as follows. The sensors keep switching the circuit one after the other in a cyclic manner with a frequency of 'F'. But when a threat of a particular type is sensed by a detector, it broadcasts this knowledge to the surrounding detector(s) (within a predetermined distance from itself). Upon receiving this information, these surrounding detector(s) stop the cyclic switching and start switching ON the circuit of the reported type of threat with

an increased frequency 'a × F' (a>1) for a predetermined period. The limit on the time of this hyperactivity is imposed so that the system can revert back to the original state once the threat is detected. Once a detector detects and reports a threat, it refrains from switching any circuit for a predetermined amount of time. By this, it avoids reporting the same detection again for this period of time, after which it is expected to have moved outside the range of the threat.

3.4.2. Application of the Learning and Memory Mechanism. When the detectors allocate equal number of time-slices to all the sensor circuits present inside it, an equal expectation is assigned to each type of threat. Practically it is very well possible that some threats are more expected than others depending on the location where the system is deployed. In such scenarios the time-slices allocated to the least expected threats are wasted. In contrast to the clonal selection mechanism, in which the detectors allocate more time-slices only to the reported type of threat for a short period of time, learning and memory mechanism allocates more time slices to the threats for a longer period of time. Also, instead of increasing the time-slices of just one type of threat, the threats are allocated time-slices in proportion to their expected probability of occurrence.

One possible mean to implement such mechanism is if the observer can keep a history of the threats found in a certain area in the past. When a detector enters a particular area, it can be updated with the history of the threats found at that area in the past. After weighing the probability of occurrence of the types of threats in the past, the detector can proportionally allocate a number of time-slices to them. Also once a type of threat is found by any detector in a particular area, more number of time-slices can be allocated to it by all detectors present in that area till they move out of it. This will reduce

the mean detection time of the more expected type of threats by emulating the 'immunological memory' feature of the human immune system.

4. EXPERIMENTAL SETUP AND SIMULATION SYSTEM

The required statistical data for parameters such as detection time, true alarms, false alarms etc. can only be obtained through experiments. Using real world experiments consisting of physical devices and people is not only time consuming and costly but highly inconvenient in terms of the required physical effort. Using computer programs which simulate the real world not only saves time and physical effort but also makes modifications to the setup easy. Part of this research was to identify the agent-based modeling packages, determine their suitability and then develop a simulation system which replicates the real world scenarios.

The HIS consists of a large number of antigens and antibodies which interact with each other producing a variety of results. Such scenarios, in which a large number of individual agents, although having predictable behavior themselves, interact with each other, produce system level outcomes that are inherently complex to study and to model. Individual-based modeling [32] is a technique in which complex systems are modeled from bottom-up, in turn providing relationships between the participating agents and the system level behavior which emerges from their interactions. A similar approach was used in which the detectors and the threats were modeled as individual agents and their behaviors remained unchanged throughout the experiments. The detectors and sensors were made to interact with each other in a simulated environment and the system level outcomes were recorded and studied. Several agent-based modeling software packages are currently available [6]. For the following results NetLogo and MASON [31] were used as the agent-based modeling packages. MASON has a library core in Java which

facilitates discrete-event multi-agent simulation environment. Custom made simulations can be programmed and run.

The following section gives a complete list of tools and software applications used during this research.

4.1. TOOLS AND SOFTWARE

The programming environment consisted of the following tools and resources:

- NetLogo 4.0.3 : NetLogo is a cross-platform multi-agent programmable modeling environment.
- MASON Simulation Library: MASON is a fast discrete-event multiagent simulation library core in Java, designed to be the foundation for large custom-purpose Java simulations, and also to provide more than enough functionality for many lightweight simulation needs
- NetBeans 6.7 : Netbeans is a Integrated Development Environment and was used in this research to develop Java codes using the MASON Simulation library.
- Java Development Kit (JDK 5)
- Java Runtime Environment (JRE 1.5)
- MATLAB

Earlier simulations were programmed in NetLogo 4.0.3. NetLogo is a programmable modeling environment for simulating natural and social phenomena. The tool is written in Java and is particularly well suited for modeling time evolution and analysis of multi-agent complex systems. NetLogo has its own unique syntax but is very similar to objective-C. Modelers can give instructions to hundreds or thousands of 'agents' all operating independently by defining appropriate individual level behaviors

for interaction. This makes it possible to explore the connection between the micro-level behavior of individuals and the macro-level patterns that emerge from the interaction of many individuals. Comprehensive information about the tool is available at the following location. http://ccl.northwestern.edu/netlogo. Figure 4.1 shows NetLogo GUI development for the current application.

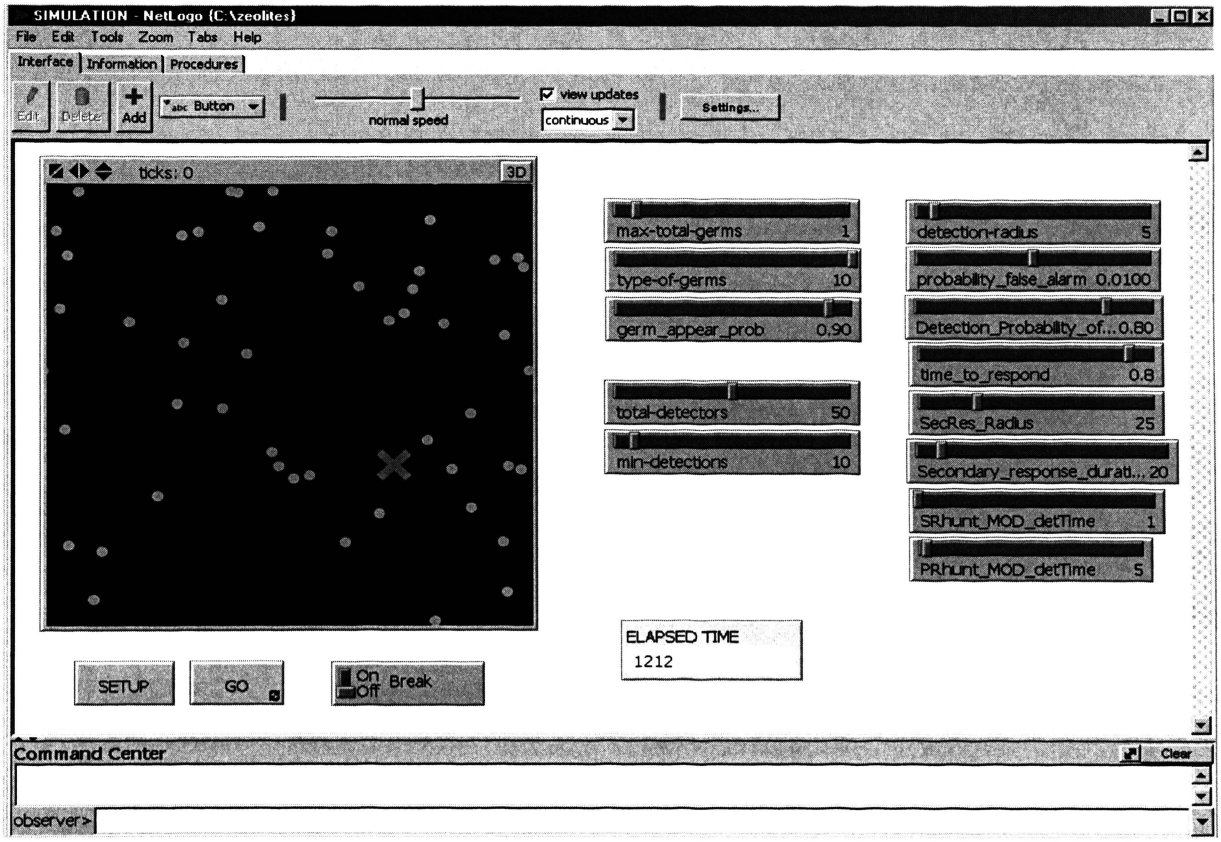

Figure 4.1. NetLogo GUI

The variables involved in the simulation can be changed with the help of sliders. The simulation can also be viewed graphically as shown while the speed of the

simulation can be varied. The green circles seen are detectors while the red-cross is the CB-agent. The program writes the values of the relevant parameters directly to a file (of type .csv). After the simulation is over the values can be read from this file into MATLAB for further analysis of the results.

NetLogo was used in developing simulations containing only a single type of CB-agent. One of the strategies developed during this research required one 2-D matrix to be used for each type of CB-agent. NetLogo provides only a single 2-D matrix. For simulations involving multiple types of CB-agents a modeling package was needed which could provide more than one 2-D matrices. MASON is another agent-based modeling software in which the simulation programs are written in Java. Thus it is possible to program more than one 2-D matrices for the simulations using the MASON library. The code is to be written in a .java file and then it can be run either in the MASON software package or in a Java IDE like NetBeans or Eclipse. It contains an optional suite where the simulation programmed in the .java file can be visualized in a 2-D or 3-D environment. The programs for this research were developed in NetBeans 6.7 IDE while using the MASON library core. Initial simulations were run on a single-core desktop computer but subsequent simulations were run on a cluster computer. The cluster computer had 4 dual-core Intel processors and multiple simulations were kept running in order to reduce the overall time required to obtain the results. Figure 4.2 shows a snapshot of the simulation programmed developed in NetBeans 6.7 IDE.

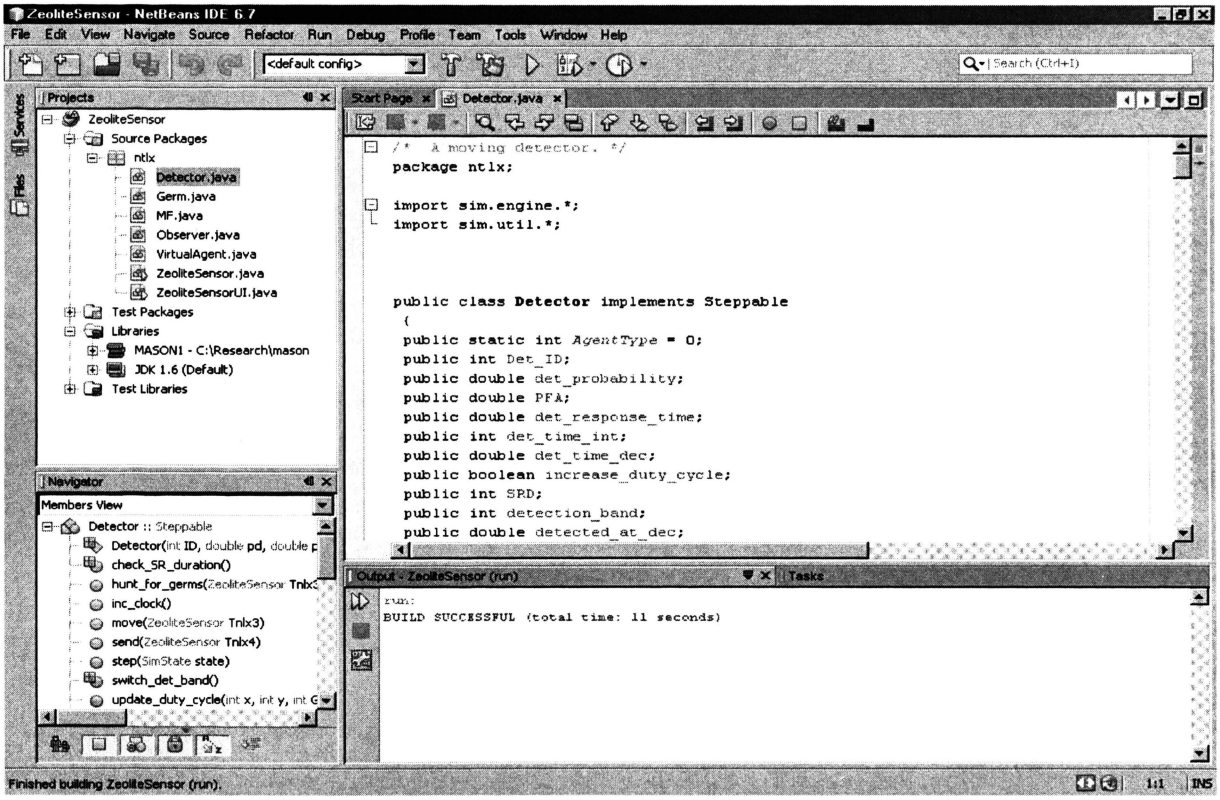

Figure 4.2. Simulation Developed in NetBeans 6.7 IDE

4.2. IMPLEMENTATION DETAILS

The entire simulation was implemented using the agent-based modeling concepts. Different types of agents were introduced into the simulation as seen in the left sector. Each agent was completely characterized in terms of its behavior. Each agent had parameters, values for which were set before the simulation started. In the simulation the detectors and CB-agents interacted with each other in an area of 27,225 (165mx165m) square meters. The detectors were able to detect 10 different types of threats and had a detection radius of 1 meter. The distance up to which the clonal response was limited was kept to be 23 meters while the population of clonal selection lasted for 29 seconds. The

detectors stopped detecting for about 5 seconds after they reported a CB-agent. The processing time of the detectors i.e. the time lag in detection and reporting was set at 800msec.

Following is a description of the all the agents used in the simulation.

4.2.1. A Detector. A detector is an agent which moves around the field while searching for CB-agents. It is capable of detecting more than one type of CB-agent and has a dedicated sensor circuit for each type of threat. At any given time the detector enables only one circuit and switches the circuits routinely in a cyclic manner. Upon sensing a CB-agent it reports the type of the CB-agent as well as its x-y coordinates in the field to the observer and also sends a message to its surrounding detectors about the type of the CB-agent it detected in order for them to activate the clonal selection mechanism.

Following are the parameters associated with the detector model:

1) Probability of detection: This is the probability that the sensor gives an alarm when the CB-threat is actually present within its detection range.
2) Probability of false alarm: This is the probability that the detector gives an alarm in absence of the CB-agent.
3) Response time: This is the processing time of the detector i.e. the finite amount of time that the detector takes for detecting the CB-agent and reporting it to the observer.
4) Boost duty cycle: This is a boolean value which is set once the detector gets a message from any of its surrounding detectors. If this value is true, the detector activates its clonal selection mechanism.
5) Clonal selection duration: This is the amount of time for which the clonal

selection is kept activated by the detector.

6) Clonal selection radius: This is the distance within which the detector sends out a signal to other detectors to activate their clonal selection mechanism.

7) Detection bands: This is the total number of types of CB-agents the detector is able to sense.

8) Detector mute time: This is the amount of time for which the detector stops reporting CB-agents after it has sensed it. This avoids multiple reporting from the same detector and facilitates getting reconfirmations from distinct detectors.

9) Detector clock: This is the detector's internal clock. The detectors clocks are not synchronized with each other.

The average moving speed of the detectors was set to 1 meter per second and on average changed their direction after taking about 10 steps. Here the detectors randomly picked an angle of rotation from $45n$ (n= 1 to 8). It is important to note that these two parameters have a significant impact on the detection time.

4.2.2. A CB-threat. The CB-threat can occur anywhere in the field. Each CB-agent has a specific type. They are persistent until detected. Once detected, they are removed from the system.

4.2.3. The Observer. This is the central monitoring and decision making station and in the real world it can be located far away from the site. All the detectors report to the observer about the type of the CB-agent that they detect and their position in the field. The observer processes the data reported to it by the detectors and declares a system level detection taking into consideration the physical location from where the reporting was

made. A system level detection is declared when the detection threshold M for any type of threat is reached. The observer maintains its own time counter. The observer also maintains one 2-D matrix per type of CB-agent that the detectors are capable of sensing.

4.2.4. The Virtual Agent. This agent is introduced for simulation purposes only and will not be present in the real world scenarios. This agent performs all the simulation related tasks. It performs the following tasks:

1) Placing the CB-agents in the field.
2) Removing the CB-agents after they have been detected.
3) Keeping a count of the total CB-agents placed and detected.
4) Keeping a note of the position where each CB-agent was placed
5) Keeping a track of time since the CB-agents were placed.
6) Keeping a count of the true alarms and false alarms.
7) The time-to-detection for CB-agents.

5. ANALYTICAL MODELS

5.1. RANDOM-HOP

In order to verify the programmed simulation environment and to ascertain the desirable functioning of the random number generator used in the agent-based software packages, analytical models were developed and compared to the simulation results. For more complex schemes in which detectors follow brownian type of motion, analytical models are extremely difficult to work out. Thus, the analytical models for simple schemes where detectors follow the random-hop type of movement were developed and compared with the simulation results.

Note that at this time it is assumed that there is only one type of CB-agent present and all detectors are only sensing for that particular type. Also there is only one CB-agent at a fixed location at any given time.

Let p be the probability that a detector will detect a CB-threat at any time step. Detectors are independent of each other from one time step to the other. However, the probability p is conditioned on the existence of the CB-threat in the world. Thus:
when a CB-agent is present,

$$p = \frac{\pi r^2}{A} p_d + p_{fa} \tag{1}$$

when the CB-agent is not present,

$$p = p_{fa} \tag{2}$$

Let t be the time since the occurrence of CB-agent (when it is placed) or the time since the start of simulation if no CB-threat is present. If p is the probability of a detection response from a detector at any given time step, the probability of at least one detection response from a detector in time t is given by:

$$p_t = 1 - (1 - p)^t \tag{3}$$

Also the probability of at least M detectors to respond within one time step is given by:

$$P(M) = 1 - B(M - 1, N_d, p) \tag{4}$$

where $B(i, N_d, p)$ is the binomial CDF.

The probability of M detectors to have detected the CB-threat at the end of time t is given by:

$$P_t(M) = b(M, N_d, p_t) \tag{5}$$

where $b(i, N_d, p)$ is the binomial PDF.

Now, the probability of at least M distinct detectors to have detected the CB-threat in time t is given by

$$P_M(t) = \sum_{i=0}^{M-1} P_{t-1}(i)\, P(M-i) \tag{6}$$

The mean time for detection for N_d detectors for a system level call of detection after M independent conformations can be approximated as:

$$\mu(M) = \sum_{t=0}^{\infty} t\, P_t(M) \approx \frac{M}{pN_d} \tag{7}$$

thus, the case where $p_d = 1$ and $p_{fa} = 0$, the mean response time is given by

$$\mu(M) \approx \frac{MA}{\pi r^2 N_d} \tag{8}$$

The preliminary results for simulated experiments were observed to be consistent with the analytical estimate. Following are some of the plots showing the effect of change in values of various parameters on the probability density function (PDF) of the time-to-detection. The curve in blue is the histogram of the detection time obtained from 500 NetLogo simulations while red curve is the analytical PDF based on equation 6. The simulated values in these graphs show high variance since only 500 observations are used to draw the PDF. For all cases the world size A is 27,225 square meters.

Figure 5.1 and Figure 5.2 show the comparison for two different values of radius of detection r. The response time reduces by the square of the detection radius. The analytic PDF and simulated response time show close agreement. The analytical mean

response time for the case of r=5 and r=10 with N_d =100 and M = 10 is 34.5 and 8.6 respectively.

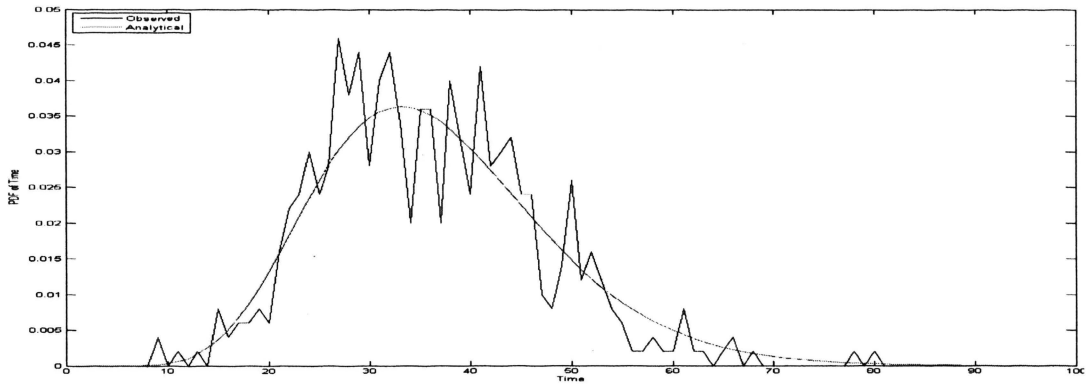

Figure 5.1. PDF for r=5 and N_d=100, M=10, P_d=1, P_{fa}=0, P_{ep}=1

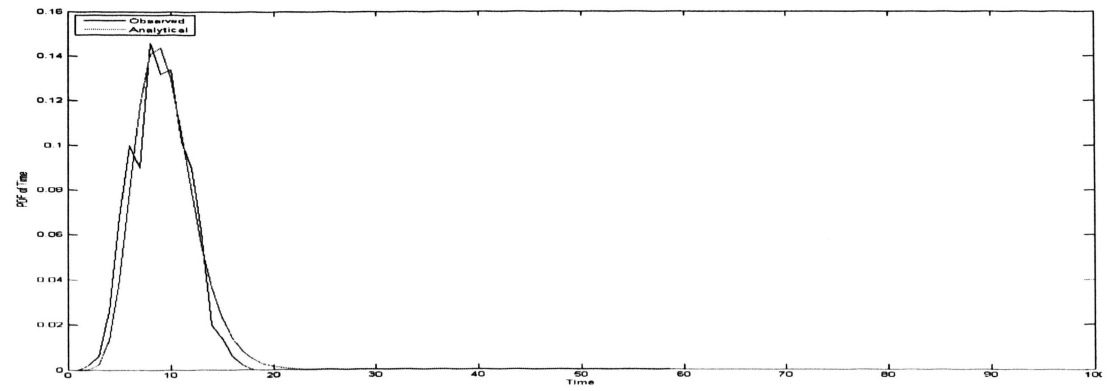

Figure 5.2. PDF for r=10 and N_d=100, M=10, P_d=1, P_{fa}=0, P_{ep}=1

Figure 5.3, Figure 5.4 and Figure 5.5 show the comparison for three different values for the number of detectors in the world (N_d). The response time reduces linearly with the number of detectors. The analytic PDF and simulated response time again shows

close agreement for all cases. The analytical mean response time for the three case of N_d = 25, N_d = 50, N_d = 100 with r=10 and M = 10 is 34.5, 17.3 and 8.6 respectively. Figures 5.6, Figure 5.7 and Figure 5.8 show the comparison for different values of the number of detection threshold M while Figures 5.9, Figure 5.10 and Figure 5.11 show the comparison for different value of probability of detection P_d.

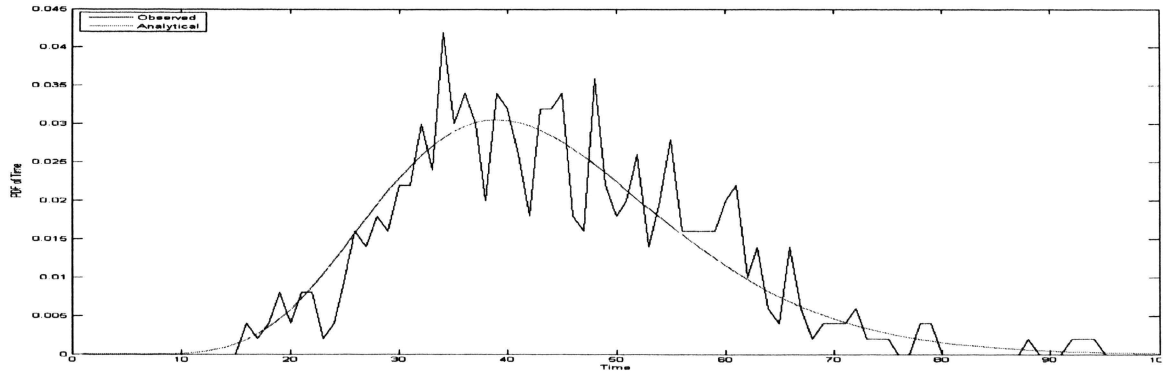

Figure 5.3. PDF for N_d=25 and r=10, M=10 , P_d=1, P_{fa}=0, P_{ep}=1

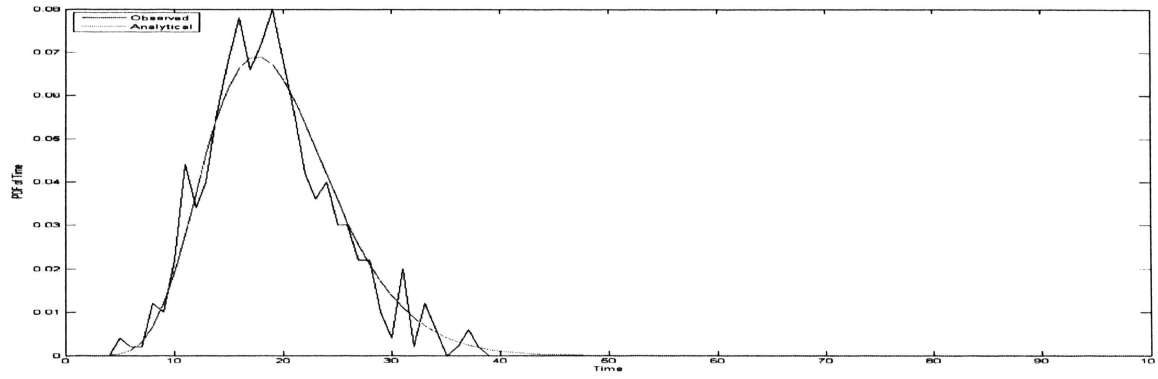

Figure 5.4. PDF for N_d = 50 and r=10 , M=10 , P_d=1, P_{fa}=0, P_{ep}=1

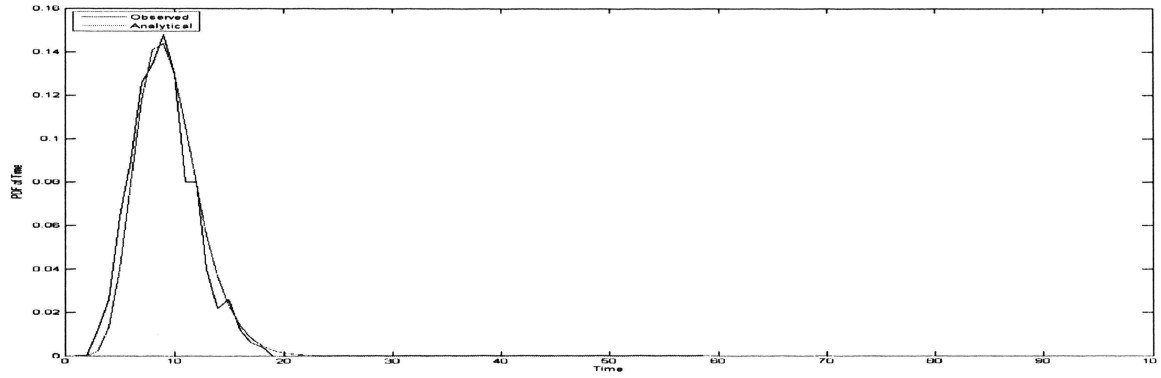

Figure 5.5. PDF for N_d = 100 and r=10 , M=10 , P_d=1, P_{fa}=0, P_{ep}=1

Figures 5.6, Figure 5.7 and Figure 5.8 show the comparison for different value of number of detections required *(M)*. The detection time increases linearly with *(M)*.

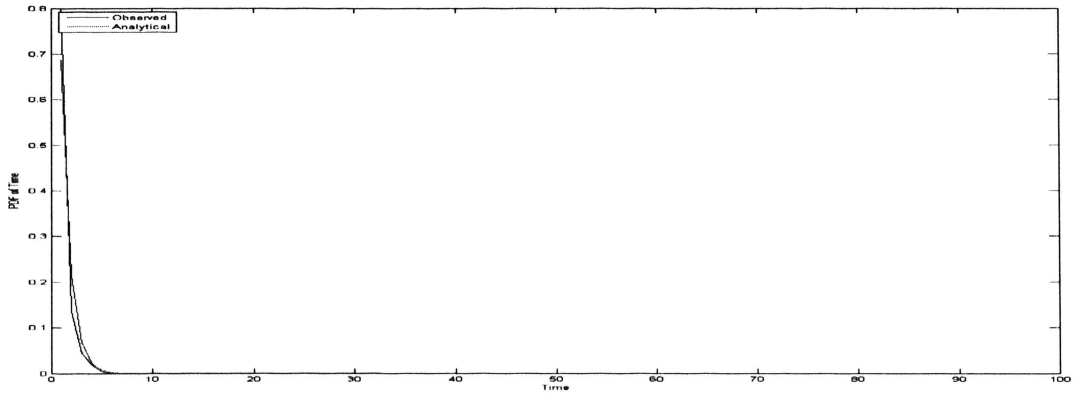

Figure 5.6. PDF for M=1 and N_d =100, r=10, P_d=1, P_{fa}=0, P_{ep}=1

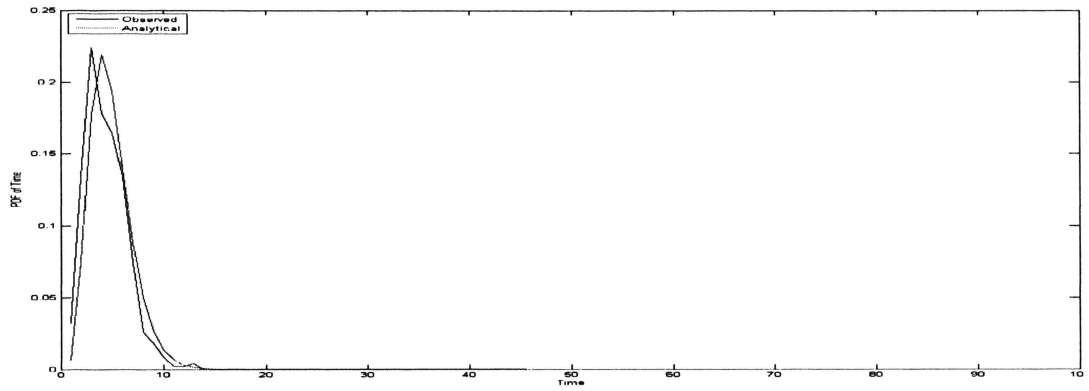

Figure 5.7. PDF for M=5 and N_d = 100,r=10, P_d=1, P_{fa}=0, P_{ep}=1

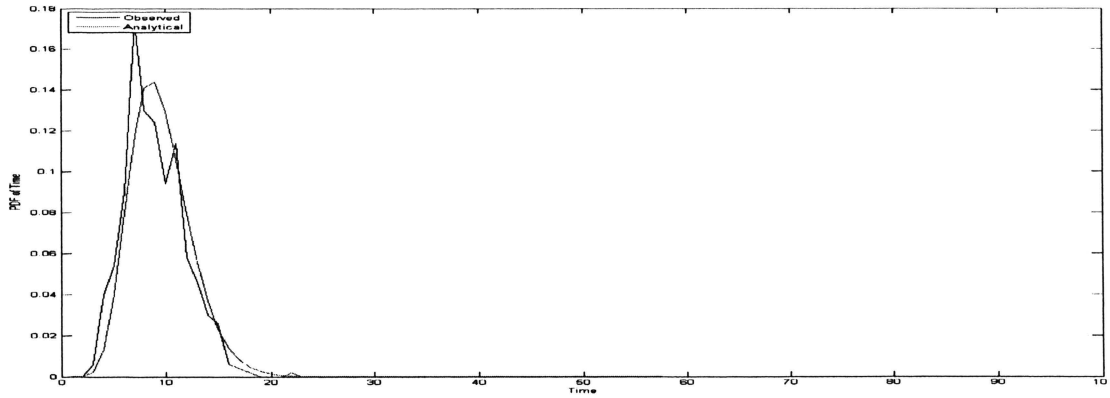

Figure 5.8. PDF for M=10 and N_d = 100,r=10, P_d=1, P_{fa}=0, P_{ep}=1

Figures 5.9, Figure 5.10 and Figure 5.11 show the comparison for different value of probability of detection P_d. The detection time decreases linearly with increase in the values of P_d.

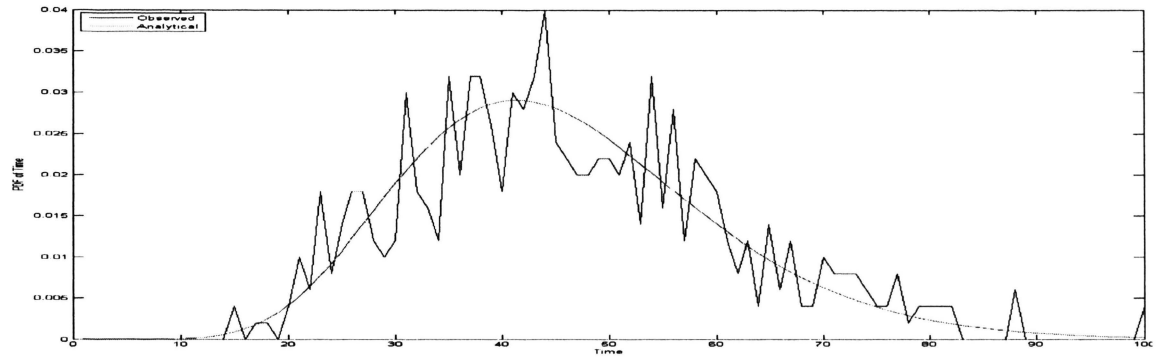

Figure 5.9. PDF for P_d=0.2 and N_d = 100,r=10, M=10, P_{fa}=0, P_{ep}=1

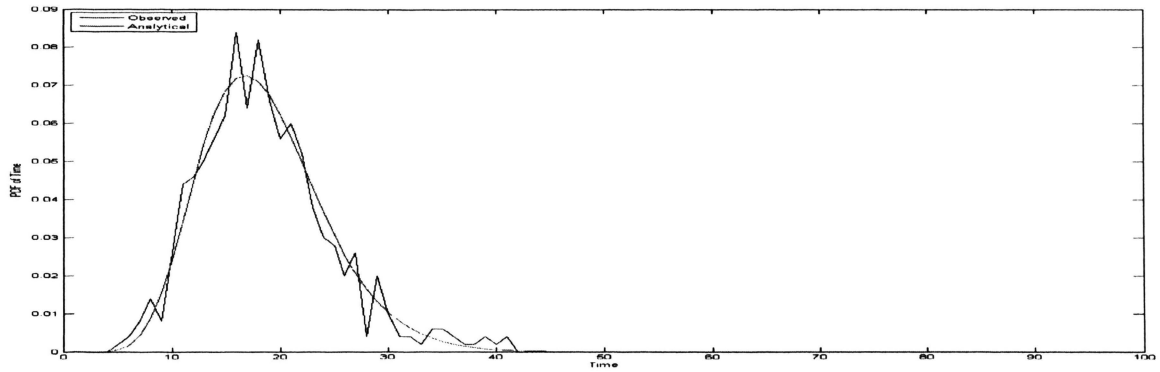

Figure 5.10. PDF for P_d=0.5 and N_d = 100,r=10, M=10, P_{fa}=0, P_{ep}=1

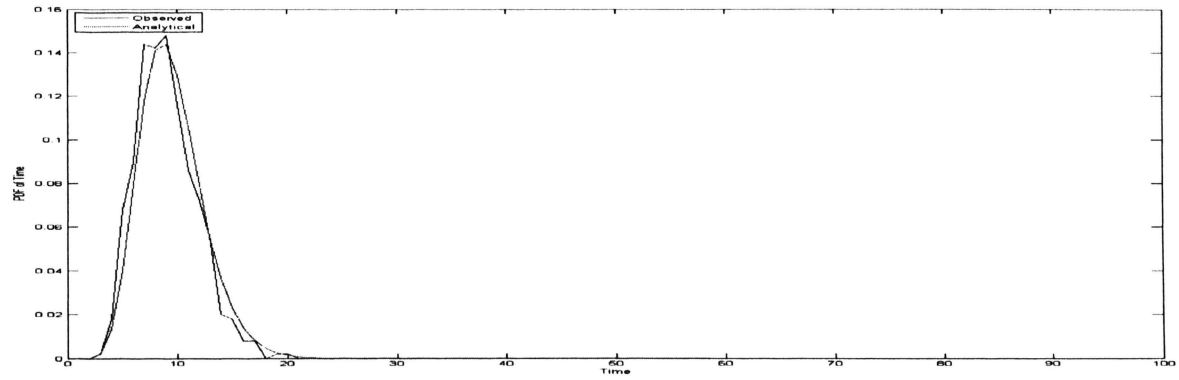

Figure 5.11. PDF for P_d=1 and N_d=100, r=10, M=10, P_{fa}=0, P_{ep}=1

5.2. CLONAL SELECTION USING RANDOM-HOP TYPE OF MOTION

For scenarios in which the detectors follow brownian type of motion, the analytical model for the detection time with the clonal selection is extremely complex just as in the scenarios without clonal selection. The model is simpler in case where detectors randomly jump from one place to another in the field. The detection time in this case is the lower limit of the achievable detection time. With the introduction of Brownian motion the detection time increases since the detectors take longer time to move from one place in the field to another.

Following equations summarize the clonal selection strategy for random-hop motion in absence of false alarms.

Let p_1 be probability of detection during primary response, then,

$$p_1 = \frac{\pi * R^2}{g * A} \tag{9}$$

Let p_2 be probability of detection during clonal selection mechanism, then,

$$p_2 = \frac{\pi * R^2}{A} \tag{10}$$

Probability that a single detector first detects at time s ($1 \leq s \leq t\text{-}1$) is :

$$P_d(s) = p_1 * (1 - p_1)^{s-1} \tag{11}$$

Probability that a detector does not detect in *t-s-1* seconds during the clonal selection mechanism is

$$a = (1 - p_2)^{t-s-1} \tag{12}$$

Probability that there is no detection in *s* seconds during the primary response

$$b = (1 - p_1)^s \tag{13}$$

Thus, probability that the first detection occurs at time = *s*

$$P(s) = \sum_{i=1}^{R} \binom{R}{i} * P_d(s)^i * (1 - a)^{R-i} * b^{R-i} \tag{14}$$

where ($1 \leq R \leq M-1$)

Thus, Probability that *M* detections occur in time *t* is given by

$$P(t) = \left(\sum_{R=1}^{M-1} \sum_{s=1}^{t-1} \binom{N}{R} * P(s) * (1 - p_1)^{s*(N-R)} * (1 - p_2)^{(t-1-s)*(N-R)} * \right.$$
$$\left.(1 - B(M - R - 1, N - R, p_2))\right) + \left((1 - p_1)^{N*(t-1)} * (1 - B(m - 1, N, p_1))\right) \tag{15}$$

For primary response, the equation is the same as equation (4) except the probability of detection for each detector is

$$p = \frac{\pi * R^2}{g * A} \tag{16}$$

Figure 5.12. shows the comparison of simulation and analytical results for the clonal selection model. As indicated by Figure 5.12., the analytical results match with the simulation results.

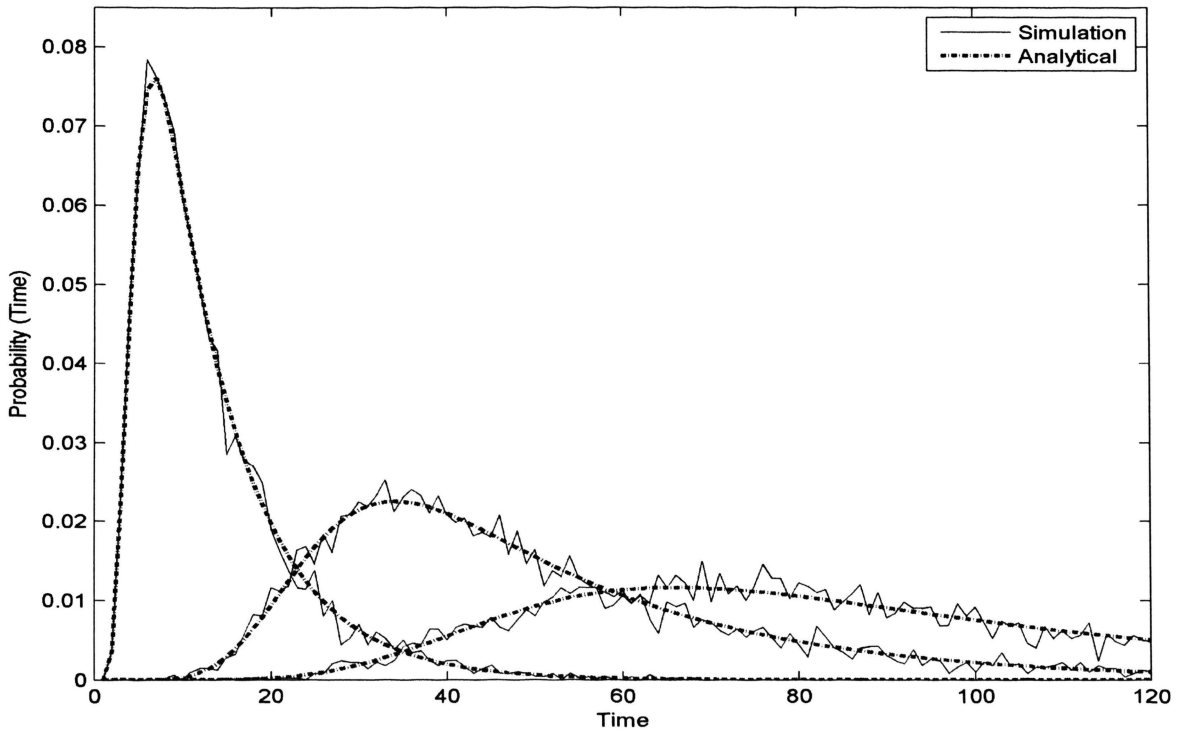

Figure 5.12. Comparison of Simulation and Analytical Results

5.3. EFFECTIVENESS OF CLONAL SELECTION MODEL

Figure 5.13 shows the comparison of PDFs for time-to-detection with and without clonal selection mechanism for N_d=100, M=5, R=5 and g=10.

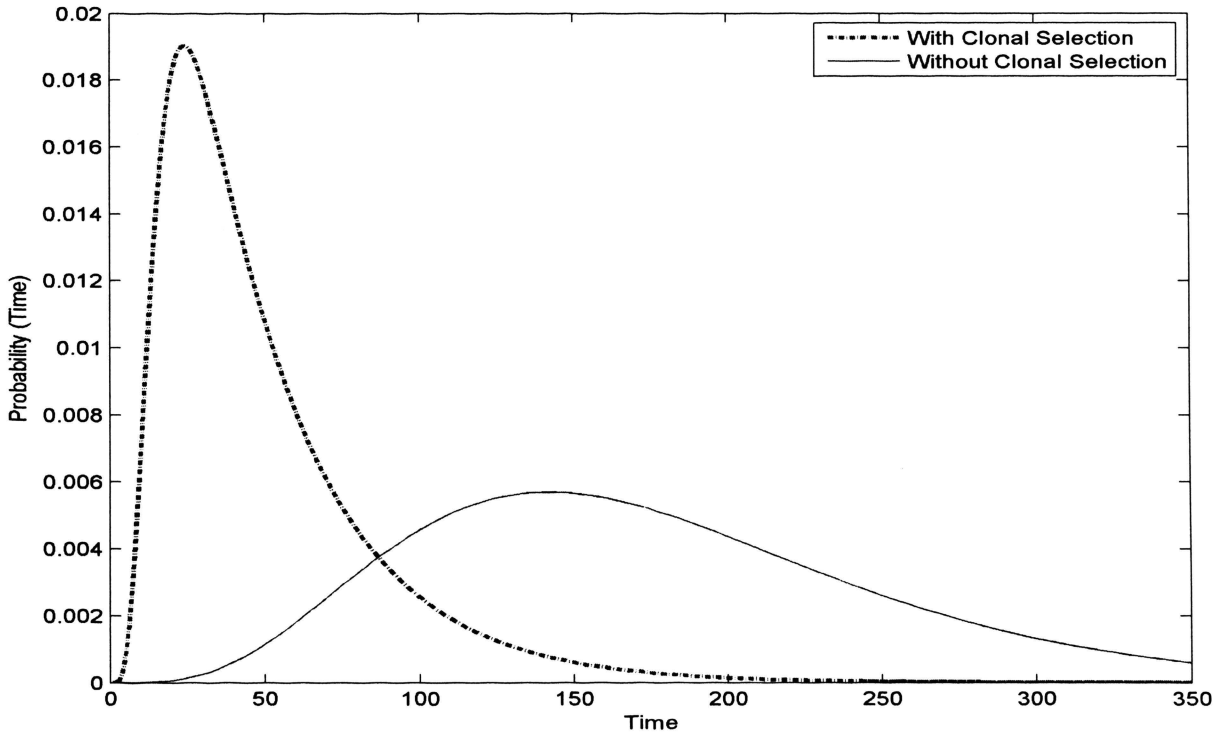

Figure 5.13. Comparison of PDFs of Detection Time for Simulations With and Without the Clonal Selection Mechanisms

As can be clearly observed, the PDF in case of simulations with the clonal selection is concentrated near lower values of detection time. Table 5.1 and 5.2. show the change in percent savings time for increasing values of types of threats that the detector can detect and detection threshold respectively, as derived from analytical equations derived earlier for random-hop motion of detectors. The percent savings in time

decreases as motion of the detectors approaches the Brownian type of motion. As can be observed, the percent savings time increases with the values of types of threats detected by the detectors and the detection threshold.

Table 5.1. Percent Savings in Time for Increasing Values of Types of Threats the Detectors Can Detect for N_d=80, M=6, R=6.

Type of threats the detectors can detect (g)	w/ Clonal Selection (seconds)	w/o Clonal Selection (seconds)	Percent savings in time (%)
2	22.38	36.12	38.04
5	31.56	90.31	65.05
10	46.66	180.63	74.16
15	61.71	270.94	77.22
20	76.60	361.26	78.79
25	90.90	451.58	79.86
35	115.76	632.21	81.68
50	140.81	903.16	84.40
70	155.48	1264.43	87.70
85	158.00	1535.38	89.70
100	156.63	1806.33	91.32

Table 5.2. Percent Savings in Time for Increasing Values of Detection Threshold (M) for N_d=80, R=6, g=10.

Detection Threshold (M)	w/ Clonal Selection (seconds)	w/o Clonal Selection (seconds)	Percent savings in time (%)
2	34.11	60.21	43.34
3	37.17	90.31	58.83
4	40.29	120.42	66.53
5	43.45	150.52	71.12
6	46.66	180.63	74.16
7	49.91	210.73	76.31
8	53.20	240.84	77.90
9	56.54	270.94	79.13
10	59.92	301.05	80.09

6. OTHER TECHNIQUES DEVELOPED TO ASSIST THE AIS

6.1. POSITION BASED DETECTION

All the sensors are prone to give false alarms anywhere in the field. In case of a threat present at point x-y in the field, a true alarm is expected at and around that point only, or in other words, sensors are expected to give true alarms very close to the location of the threat. All the other alarms given at any other place in the field can be identified as false alarms. These false alarms add up very quickly resulting in higher values of system level FARs.

Following technique was developed to implement a position based detection strategy to mitigate these FARs.

1) For a rectangular field having length: x and breadth: y, the observer maintained a matrix (called threat-matrix) having x-rows and y-columns. One such matrix was assigned to every type of CB-Threat. For example, for a total detection capability of 10 types of CB-threats, the observer maintained 10 corresponding matrices. All elements were initialized to zero.
2) An element x-y in the matrix, represented the corresponding physical location in the field. A detector, upon sensing a type of threat, reported it to the observer along with its location x-y at that instant.
3) The observer, after receiving this reporting of the type of threat, would increment by one, the element x-y, and also the surrounding elements within a distance equal to detection-radius in the matrix corresponding to that type of threat. The observer would carry out the same procedure for every reporting. Thus the value of an element (called confidence level) in the matrix represented

the total number of reportings at that physical location.

4) If the value of any element was found to be greater than or equal to the threshold *M*, the observer would declare that the corresponding CB-threat was present at that location.

5) After such a declaration, the matrix element at that location and the elements surrounding it are reset to zero.

With the above strategy, false alarms generated by detectors at distant locations were naturally ignored. A system false alarm was possible only if detectors reported a false alarm of the same type of threat at the same location in the field which is less likely, and thus considerably reducing the system level FAR.

6.2. DECAYING THREAT MARTIX STRATEGY

Although the detector-position based strategy described in the previous section considerably reduces the system level FAR, false alarms keep accumulating at any given location over a longer period of time. As a result, if the simulation is running continuously and indefinitely, every location is guaranteed to give a false alarm. In order to address this issue, a Decaying Threat Matrix (DTM) strategy was developed in which the values of the elements of the threat-matrix are reduced periodically and predictably by applying a 'decay function' in order to reduce the accumulated false alarms and thus the FARs. Because of the decay function, the confidence levels build up in the threat matrix due to false alarms takes a longer time to reach the threshold value of 'M' thereby reducing FARs.

The values of elements were reduced in the following way:

$$E(x,y,time) = (e^{-\lambda}) \times (E(x,y,time-1) \quad (17)$$

where E(x,y,t) is the matrix element corresponding to location *x*-*y* at time *t*. Confidence levels build up in the matrix due to true alarms are much faster than due to false alarms. The decay factor λ is kept high enough to reduce the false alarms and low enough not to affect the true alarms.

7. RESULTS AND DISCUSSIONS

7.1. CLONAL SELECTION MECHANISM

7.1.1. Effect of Clonal Selection Mechanism on Detection Time. Figure 7.1. shows the plot of detection time Vs number of detectors N_d with M=6 and R=1 for simulations with and without the implementation of clonal selection strategy. The speed of the detectors was 1 meters per second while their detection radius was 1 meters. The plots clearly indicate the effectiveness of the clonal selection strategy showing a reduced time response in all cases.

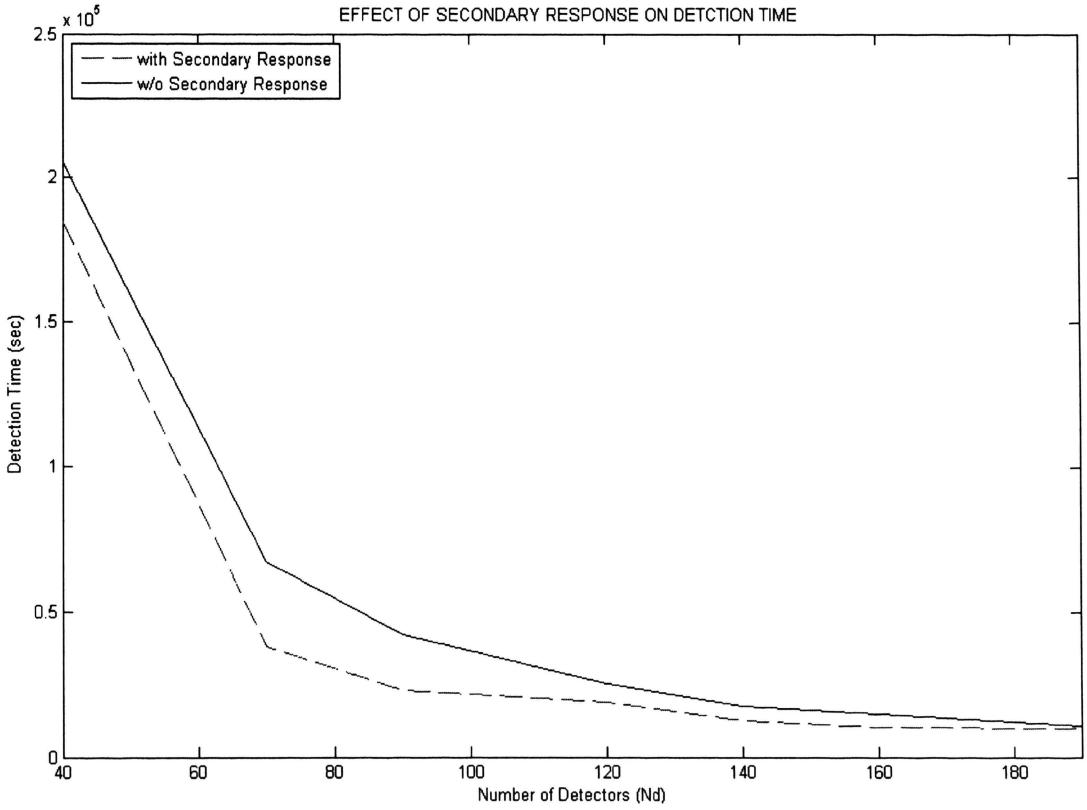

Figure 7.1. Effect of the Clonal Selection Mechanism on Detection Time, Detector Moving Speed=1 meter/sec

Table 7.1. shows percent change in the detection time after the application of the clonal selection mechanism. As indicated by the values in Table 7.1., a maximum of 45.08% reduction was seen for the given set of parameters with the help of clonal selection mechanism. There is minimum percentage change in the detection times obtained for lower as well as higher values of N_d. This is because, for lower values, there are not enough detectors near the CB-agent for the strategy to effectively work while for higher values there are already enough detectors near the threat which facilitate lower detection times even without the clonal selection mechanism because of the sheer number of detectors present at that point.

It is important to note that the effectiveness of the clonal selection mechanism depends on the speed, type of movement and detection radius of the detectors apart from the value of N_d. Lower speeds result into detectors not able to reach the point where the threat is located before their duty-cycle-boost gets deactivated.

Table 7.1. Percent Change in Mean Detection Time as a Function of N_d

N_d	Change in Mean Detection Time
40	10.02 %
70	43.4312 %
90	45.0863 %
140	30.3483 %
160	28.5479 %
190	5.8399 %

Figure 7.2. shows the plot of detection time Vs number of detectors N_d with M=6 and R=5 for simulations with and without the implementation of clonal selection strategy. The speed of the detectors was 3 meters per second while their detection radius was 5 meters.

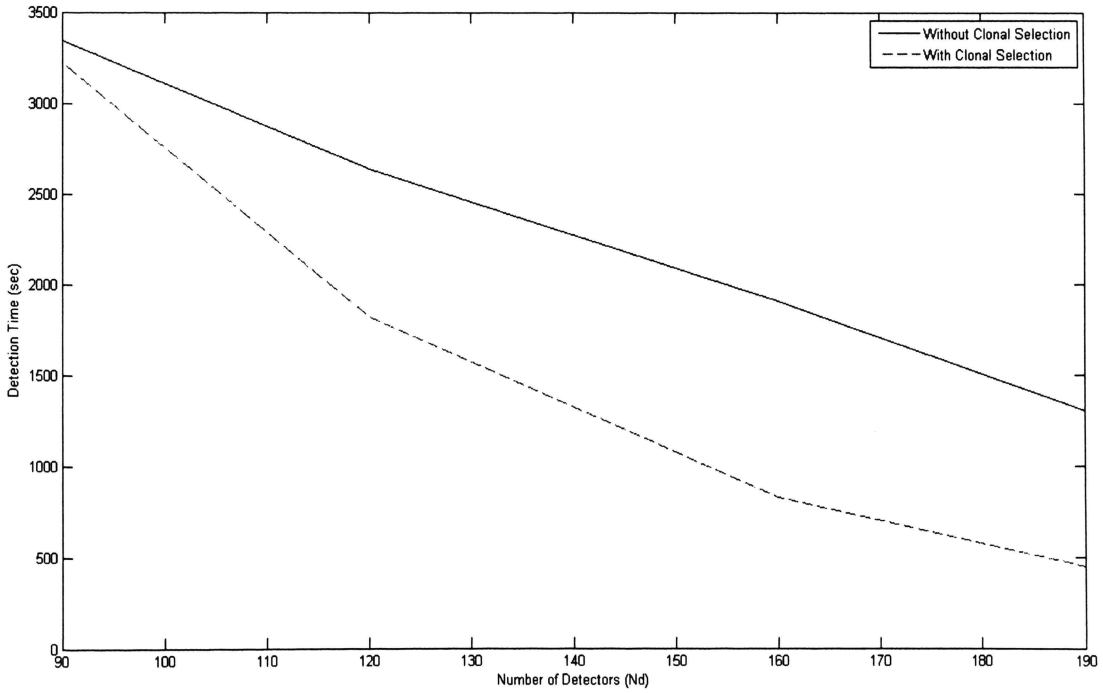

Figure 7.2. Effect of the Clonal Selection Mechanism on Detection Time, Detector Moving Speed=3 meters/sec

Table 7.2. shows percent change in the detection time after the application of the clonal selection mechanism. As indicated by the values in Table 7.2., a maximum of 65.08% reduction can be seen for the given set of parameters with the help of clonal selection mechanism.

Table 7.2. Percent Change in Mean Detection Time as a Function of N_d

N_d	Change in Mean Detection Time
90	3.59 %
120	30.91 %
160	56.59 %
190	65.75 %

7.1.2. Effect of Clonal Selection Strategy on Multiple CB-agents. Ideally, the clonal selection mechanism triggered because of one type of CB-agents should not affect the detection times for other types present in the field at that time. Figure 7.3 shows the effect of clonal selection mechanism on other CB-agents present in the field. The values of clonal selection radius and clonal selection duration were adjusted to have minimal effect on the detection time of other CB-agents present in the field. Clonal selection radius was taken as $1/16^{th}$ of the total area of the field while clonal selection duration was chosen to allow detector(s) surrounding the detector which initiated the clonal selection mechanism to reach the reported place in the field while their clonal selection mechanism still activate. The plot indicates minimal difference in the mean detection times of two types of threat placed simultaneously in the field.

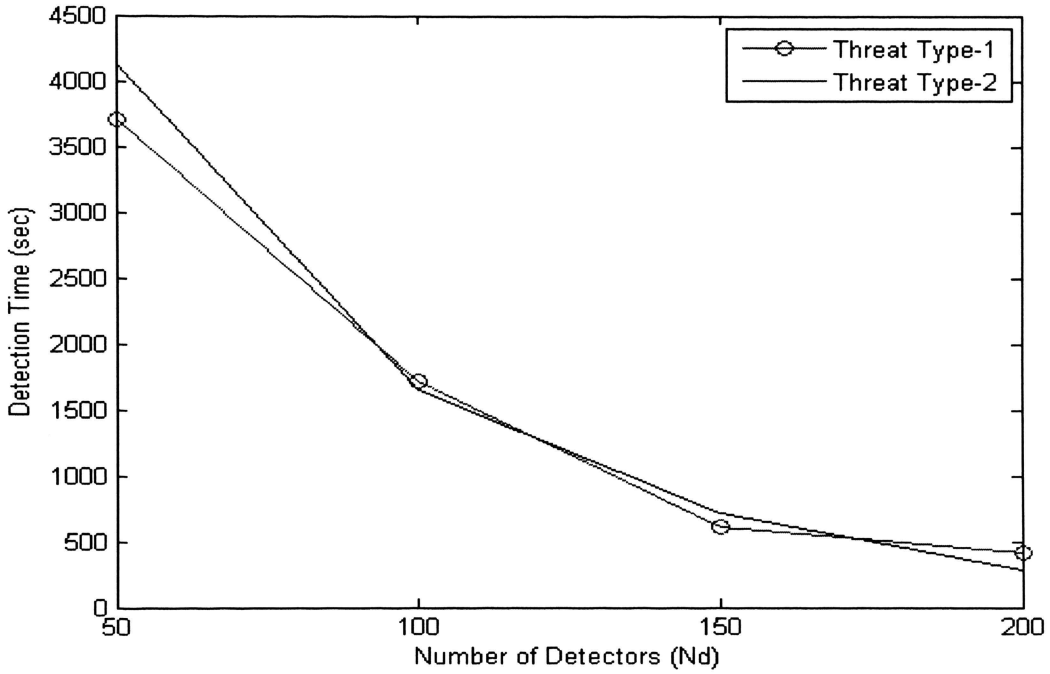

Figure 7.3. Effect of Clonal Selection Mechanism on Other CB-agents in the Field

7.2. DTM STRATEGY

Figure 7.4 shows the effectiveness of the DTM strategy. True alarms, false alarms and ratio of true alarms to false alarms are shown for three different values of the FARs of the detectors. There is minimal change in the total true alarms after the application of the DTM strategy. A considerable reduction can be seen in the false alarms after the application of this strategy, as a result of which there is a considerable increase in the ratio of true alarms to false alarms after the application of the DTM strategy. This ratio reduces proportionally with an increase in the values of the FARs of the detectors.

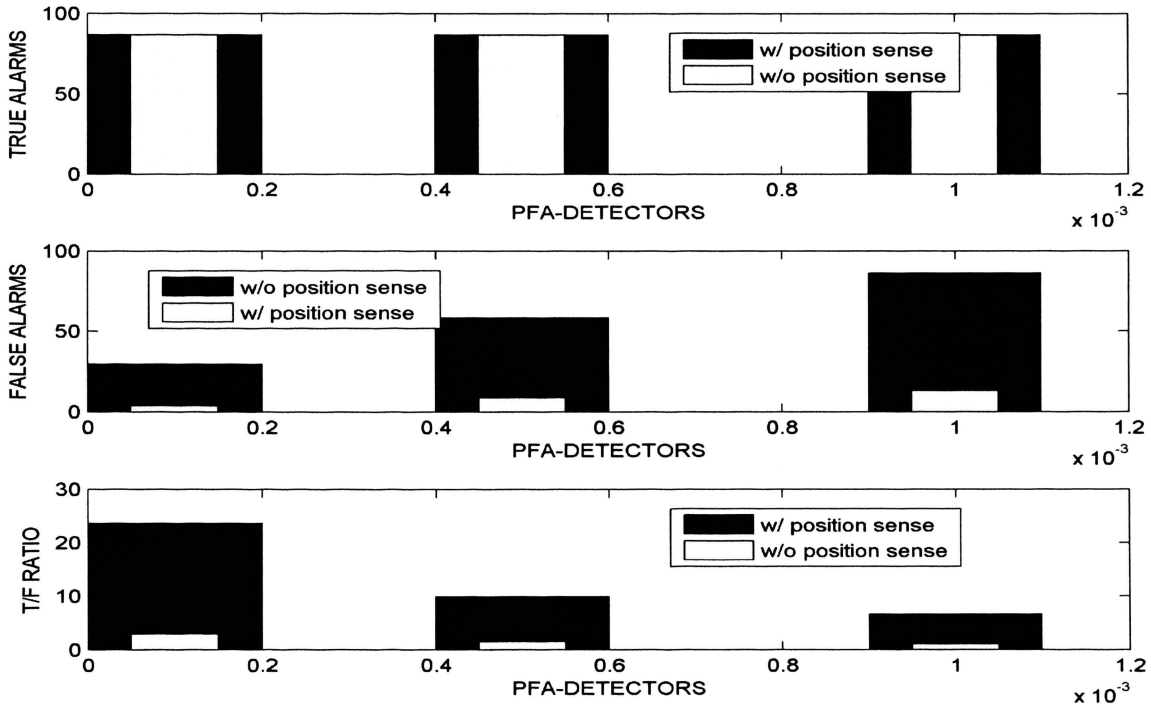

Figure 7.4. True Alarms, False Alarms, T/F Ratio for the DTM Strategy

Table 7.3 corroborates the effectiveness of the DTM strategy. While the mean detection time for the true alarms is increased, the false alarm rate is significantly reduced by implementing the DTM strategy. One reason for reduced detection time in case when DTM is not implemented is also the fact that there are residual false detections present at all locations so that when the actual threat is introduced, it can be detected faster. However, for the same reason there were more false alarms as well. With an increase in the detection threshold *M,* there is a proportional increase in the percentage reduction of the false alarms as well as the detection time, as a result of which a tradeoff has to be realized.

Table 7.3. Increase in Mean Detection Time and Percent Decrease in FAR w.r.t. M

	Mean Detection Time (sec)		FAR (per day)		
M	w/ DTM strategy	w/o DTM strategy	w/ DTM strategy	w/o DTM strategy	% Reduction
2	747	440	1795.5	4655.1	61.42
3	1031	625	624.2	3018.1	79.31
4	1619	734	219.5	2098.7	89.54
6	2971	793	21.95	1305	98.31
8	5501	971	2.35	927.55	99.74
10	9462	1237	0.15	684.24	99.97

7.3. P_d AND FAR AS A FUNCTION OF N_d

Tables 7.4, Tables 7.5, Tables 7.6 and Tables 7.7 show the ratio of FAR/P_d for different values of P_d and P_{fa}. Ideally the FAR/P_d should be zero. As can be observed, with increasing values of the number of detectors *(N_d)*, there is a simultaneously increase in the values of P_D and FAR. Similarly, with increasing values of the detection threshold (*M*), there is a simultaneously decrease in the values of P_D and FAR. A tradeoff between the achievable values of P_D and FAR is thus necessary.

Table 7.4. P_D and FAR as a function of N_d , M=3, P_d=0.75

N_d		40	60	80	100	120	140	180	200
P_{fa} =0.0001	P_D	0.03	0.06	0.06	0.11	0.25	0.45	0.51	0.76
P_{fa} =0.001	P_D	0.13	0.2	0.29	0.38	0.4	0.62	0.78	0.82
P_{fa} =0.01	P_D	0.79	0.86	0.9	0.93	0.98	0.97	0.99	0.95
P_{fa} =0.0001	FAR (per day)	0.02	0.03	0.27	0.42	0.58	0.85	1.40	1.84
P_{fa} =0.001	FAR (per day)	4.16	8.92	15.43	23.42	30.45	39.14	58.25	69.79
P_{fa} =0.01	FAR (per day)	141.88	395.9	681.2	1092.0	1575.1	2102.9	3199.2	3865.5
P_{fa} =0.0001	FAR/P_D	0.66	0.5	4.5	3.81	2.32	1.88	2.74	2.42
P_{fa} =0.001	FAR/P_D	32	44.6	53.2	61.63	76.12	63.12	74.67	85.1
P_{fa} =0.01	FAR/P_D	179.5	460.34	756.8	1174.1	1607.24	2167.9	3231.5	4068.9

Table 7.5. P_d and FAR as a function of M, N_d=100, P_d=0.75

M		2	3	4	5	6	7	8	9
P_{fa} =0.0001	P_D	0.38	0.32	0.21	0.16	0.08	0.07	0.03	0.01
P_{fa} =0.001	P_D	0.57	0.52	0.41	0.27	0.23	0.19	0.1	0.06
P_{fa} =0.01	P_D	0.95	0.94	0.83	0.72	0.63	0.41	0.3	0.15
P_{fa} =0.0001	FAR (per day)	2.51	0.61	0.10	0.03	0	0.006	0	0
P_{fa} =0.001	FAR (per day)	49.45	27.10	16.55	11.04	6.47	3.60	1.79	0.79
P_{fa} =0.01	FAR (per day)	1892.9	1183.1	845.7	669.8	532.52	445.38	376.4	294.8
P_{fa} =0.0001	FAR/P_D	2.64	0.64	0.12	0.04	0	0.01	0	0
P_{fa} =0.001	FAR/P_D	86.75	52.11	40.36	40.88	28.13	18.94	17.9	13.16
P_{fa} =0.01	FAR/P_D	1992.5	1258.6	1018.9	930.2	845.26	1086.2	1254.6	1965.3

Table 7.6. P_D and FAR as a function of N_d, M=3, P_d=0.9

N_d		40	60	80	100	120	140	180	200
P_{fa} =0.0001	P_D	0.005	0.01	0.05	0.073	0.17	0.32	0.48	0.7
P_{fa} =0.001	P_D	0.2	0.28	0.31	0.51	0.54	0.71	0.81	0.89
P_{fa} =0.01	P_D	0.89	0.93	0.96	0.96	0.98	0.98	0.99	1
P_{fa} =0.0001	FAR (per day)	0.03	0.01	0.10	0.22	0.40	0.57	1.34	1.50
P_{fa} =0.001	FAR (per day)	3.32	8.53	13.46	22.08	31.21	39.21	58.47	67.66
P_{fa} =0.01	FAR (per day)	204.6	444.5	776.1	1207	1687.8	2158	3452.6	3890.7
P_{fa} =0.0001	FAR/P_D	6	1	2	3.01	2.35	1.78	2.79	2.14
P_{fa} =0.001	FAR/P_D	16.6	30.46	43.41	43.29	57.79	55.22	72.18	76.02
P_{fa} =0.01	FAR/P_D	229.8	477.9	808.43	1257.2	1722.2	2202	3487.4	3890.7

Table 7.7. P_D and FAR as a function of M, N_d=100, P_d=0.9

M		2	3	4	5	6	7	8	9
P_{fa} =0.0001	P_D	0.42	0.38	0.24	0.17	0.15	0.05	0.03	0.02
P_{fa} =0.001	P_D	0.63	0.57	0.4	0.39	0.25	0.21	0.16	0.07
P_{fa} =0.01	P_D	0.96	0.95	0.89	0.79	0.68	0.54	0.34	0.16
P_{fa} =0.0001	FAR (per day)	2.39	0.29	0.12	0.01	0	0	0	0
P_{fa} =0.001	FAR (per day)	48.62	26.75	16.55	10.69	6.18	3.71	1.85	0.92
P_{fa} =0.01	FAR (per day)	1964.4	1215.6	848.5	666.3	540.4	450.98	383.8	343.78
P_{fa} =0.0001	FAR/P_D	5.69	0.76	0.5	0.05	0	0	0	0
P_{fa} =0.001	FAR/P_D	77.1	46.9	41.37	27.41	24.72	17.66	11.56	13.14
P_{fa} =0.01	FAR/P_D	2046.2	1279.5	953.3	843.4	794.7	835.1	1128.8	2148.6

8. CONCLUSIONS AND FUTURE WORK

In this research an adaptive spatiotemporal control mechanism was proposed to achieve the parameters of short detection time and low power consumption which is not possible otherwise while having the broad spectrum detection capability. The HIS mechanisms which would be useful in achieving these stringent requirements were discussed. The clonal selection mechanism gave as high as 45% savings in detection times. An increase of 280% could be seen for T/F ratio with the help of position based detection technique. With the help of the decaying threat matrix strategy, a 99.97% decrease in false alarms was seen. The implementation of learning and memory mechanism of the HIS can further improve the results, especially when there is need of a broad detection spectrum. Localization of the clonal selection mechanism needs to be implemented with the help of an observer so that the detection capability of detecting other types of threats of detectors in other areas does not get adversely affected. Also the combined effect of these techniques needs to be studied to give a comprehensive measure on the effectiveness of these strategies.

BIBLIOGRAPHY

[1] "First Responders' Ability to Detect and Model Hazardous Releases in Urban Areas is Significantly Limited," Tech. Rep. GAO-08-180, United States Government Accountability Office (June 2008).

[2] Hill, H. H., J. and Martin, S. J., "Conventional analytical methods for chemical warfare agents," Pure and Applied Chemistry 74(12), 2281–2291 (2002).

[3] Laudien, R., Riebe, D., Beitz, T., and Lohmannsroben, H.-G., "Detection of Explosive Related Nitroaromatic Compounds (ERNC) by Laser-Based Ion Mobility Spectrometry," in [Proceedings of SPIE], 7116,71160T–1–71160T–9 (2008).

[4] Guicheteau, J. and Christesen, S. D., "Principal Component Analysis of Bacteria Using Surface-Enhanced Raman Spectroscopy," in [Proceedings of SPIE], 6218, 62180G–1–62180G–8 (2006).

[5] Kay, S., Xu, C., and Emge, D., "Chemical Detection and Classification in Raman Spectra," in [Proceedings of SPIE], 6969, 696904–1–696904–12 (2008).

[6] Kumar, C. and Patel, N., "Laser Based In-situ and Standoff Detection of Chemical Warfare Agents and Explosives," in [Proceedings of SPIE], 7484, 748402–1–748402–14 (2009).

[7] Fountain III, A. W., Christesen, S. D., Guicheteau, J. A., Pearman, W. F., and Chyba, T., "Long Range Standoff Detection of Chemical and Explosive Hazards on Surfaces," in [Proceedings of SPIE], 7484, 748403–1–748403–11 (2009).

[8] Lesaicherre, M. L., Paxon, T. L., Mondello, F. J., Burrel, M. C., and Linsebigler, A., "Portable Raman Instrumentation for Rapid Biological Agent Detection and Identification," in [Proceedings of SPIE], 7319, 73190C–1–73190C–12 (2009).

[9] Quinn, T. G., Gross, R. L., Ditillo, J. T., and Lagna, W. M., "Electro-Optical Technology for Remote Chemical Detection and Identification," in [Proceedings of SPIE], 2763, 41–52 (1996).

[10] Choi, M. K., Bettermann, A. D., and van der Weide, D. W., "Biological and Chemical Sensing with Electronic THz Techniques," in [Proceedings of SPIE], 5268, 27–35 (2004).

[11] Gomez, R. B. and Dasgupta, S., "Use of Hyperspectral Remote Sensing for Detection and Monitoring of Chemical and Biological Agents - A Survey," in [Proceedings of SPIE], 5584, 276–285 (2004).

[12] Shelton, M. J., Evans, S. P., Smith, P. D., Simpson, I. A., Kaye, P. H., and Clarke, J.M., "Real-Time Biological Agent Detection Using Particle Size, Shape and Flourescence Characterization," in [Proceedings of SPIE], 5617, 284–291 (2004).

[13] Xiao, H., Agarwal, S., Sarangapani, J., Tsai, H.-L., and Dong, J., "Networked Zeolite-Capacative Sensors for Distributed and Ubiquitous Detection of Chemical/Biological Threats," Tech. Rep. LWI-181048, Leonard Wood Institute Collaborative Research Program (2009).

[14] Karl, H. and Willig, A., [Protocols and Architectures for Wireless Sensor Networks], Wiley-Interscience (2007).

[15] Delves, P. J. and Roitt, I. M., "The Immune System - First of Two Parts," The New England Journal of Medicine 343(1), 37–49 (2000).

[16] Delves, P. J. and Roitt, I. M., "The Immune System - Second of Two Parts," The New England Journal of Medicine 343(2), 108–117 (2000).

[17] De Castro, L. N. and Zuben, F. J. V., "Artificial Immune Systems: Part I - Basic Theory and Applications,"Tech. Rep. TR - DCA 01/99, School of Computing and Electrical Engineering, State University of Campinas, Brazil (Dec. 1999).

[18] De Castro, L. N. and Zuben, F. J. V., "Artificial Immune Systems: Part II - A Survey of Applications," Tech. Rep. DCA-RT 02/00, School of Computing and Electrical Engineering, State University of Campinas, Brazil (Feb. 2000).

[19] Rajewsky, K., "Clonal Selection and Learning in the Antibody System," Nature 381,751 – 758 (1996).

[20] Bernardino, H. S. and Barbosa, H. J. C., [Nature-Inspired Algorithms for Optimisation], vol. 193/2009 of Studies in Computational Intelligence, ch. Artificial Immune Systems for Optimization, 389–411, Springer Berlin / Heidelberg (2009).

[21] Gao, J. and Fang, L., [Advances in Neural Networks - ISNN 2009], vol. 5553/2009 of Lecture Notes in Computer Science, ch. A Novel Artificial Immune System for Multiobjective Optimization Problems, 88–97, Springer Berlin / Heidelberg (2009).

[22] Peng, L., Peng, Y., Liu, X., Liu, C., Zeng, J., Sun, F., and Lu, Z., [Computational Science - ICCS 2007], vol. 4488/2007 of Lecture Notes in Computer Science, ch. A Supervised Classifier Based on Artificial Immune System, 355–362, Springer Berlin / Heidelberg (2007).

[23] Forrest, S., Perelson, A., Allen, L., and Cherukuri, R., "Self-nonself Discrimination in a Computer," in [Proceedings of the 1994 IEEE Symposium on Research in Security and Privacy], 202–212 (1994).

[24] Dasgupta, D. and Forrest, S., "Novelty Detection in Time Series Data Using Ideas from Immunology," in [Proceedings of the 5th IEEE International Conference on Intelligent Systems], (1996).

[25] Stibor, T., Mohr, P., and Timmis, J., "Is Negative Selection Appropriate for Anomaly Detection," in [Proceedings of the 2005 Genetic and Evolutionary Computation Conference (GECCO '05)], (321–328) (2005).

[26] Gong, M., Jiao, L., Ma, W., and Ma. J., "Intelligent Multi-User Detection using an Artificial Immune System," Science in China Series F: Information Sciences 52(12),2342–2353 (2009).

[27] Jun, J.-H., Lee, D.-W., and Sim, K.-B., "Realization of Cooperative Strategies and Swarm Behavior in Distributed Autonomous Robotic Systems using Artificial Immune System," in [Proceedings of the IEEE International Conference on systems, Man and Cybernetics 1999], 4, 614–619 (1999).

[28] Younsi, R. and Wang, W., [Intelligent Data Engineering and Automated Learning – IDEAL 2004], vol. 3177/2004 of Lecture Notes in Computer Science, ch. A New Artificial Immune System Algorithm for Clustering, 58–64, Springer Berlin /Heidelberg (2004).

[29] Dasgupta, D., Ji, Z., and Gonzalez, F., "Artificial Immune System (AIS) Research in the Last Five Years," in [Proceedings of the 2003 Congress on Evolutionary Computation (CEC '03)], 123–130 (2003).

[30] Hart, E., McEvan, C., and Davoudani, D., [Computational Intelligence], vol. 1 of Intelligent Systems Reference Library, ch. Exploiting Collaborations in the Immune System: The Future of Artificial Immune Systems, 527–558, Springer Berlin / Heidelberg (2009).

[31] Luke, S., Revilla, C. C., Panait, L., and Sullican, K., "MASON: A Multiagent Simulation Environment," Simulation 81, 517–527 (2005).

[32] Srinivasa Shivakar Vulli, Sanjeev Agarwal, "Individual-Based Artificial Ecosystems for Design and Optimization," in [Proceedings of the 10th annual conference on Genetic and evolutionary computation] (2008).

[33] Alan S. Perelson, Gerard Weisbuch, "Immunology for physicists," APS journal, Volume 69, Issue 4, Rev. Mod. Phys.69, 1219-1268 (1997).

VITA

Yatin R. Bodas was born on May 27, 1983 in Pune, India. In May 2005, he obtained a Bachelor's degree in the Department of Electronics and Telecommunication Engineering from University of Pune, Pune, India. After graduating he worked as an Electrical and Computer Engineer at Larsen & Toubro Ltd., Mumbai, India.
In August 2008, he enrolled at the Missouri University of Science and Technology to pursue a Master's degree in the Department of Electrical and Computer Engineering under the guidance of Dr. Sanjeev Agarwal. He received his Master of Science Degree in Electrical Engineering in May 2010.