Journal of Theoretical and Applied Information Technology
10th June 2016. Vol.88. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SECURING MANETs USING THE INTEGRATION OF CONCEPTS FROM DIVERSE IMMUNE THEORIES

ANASS KHANNOUS, ANASS RGHIOUI, FATIHA ELOUAAI, MOHAMMED BOUHORMA
Laboratory of Informatics, Systems and Telecommunications,
Faculty of Science and Technology of Tangier,
Abdelmalek Essaadi University, MOROCCO
E-mail: khannous@ensat.ac.ma

ABSTRACT

Mobile ad hoc network (MANET) is a dynamic and promising research domain that contributes to the development of wireless networks. MANET characteristics such as dynamic topology, open media access, wireless communication, and resource limitations introduce several security threats. The MANET security is then Vulnerable. The use of traditional security techniques cannot be directly applied for the case of MANET, hence the need to develop more suitable methods and security algorithms. Artificial immune systems have been widely used in the field of MANET security. Several immune algorithms were used and implemented as intrusion detection systems (IDS). This paper gives an overview of major immune algorithms like Negative Selection Algorithm, Clonal Selection, and the danger theory. It then describes our approach to implement an IDS based on the combination of these immune algorithms to better simulate the human defense mechanism. The proposed algorithm is named "Combined Immune Theories Algorithm" (CITA), and is implemented with the AODV routing protocol. CITA is designed to be an auto evolutionary algorithm with some learning capabilities in order to be able to recognize and exclude unknown intruders based on deviations from normal behaviors. Simulations are done using Network simulator 2 (NS2) with increasingly insertion of malicious nodes running Resource consumption attacks. Simulation results show improved performance of the proposed CITA algorithm compared to SAODV routing protocol in terms of better detection rates, low false positive detection rates, higher throughput and packet delivery ratio.

Keywords: *MANET Security, Artificial Immune System (AIS), Negative Selection Algorithm (NSA), Clonal Selection, Danger Theory, Dendritic Cell Algorithm (DCA), Intrusion Detection System (IDS).*

1. INTRODUCTION

1.1 Mobile Ad hoc Networks

Mobile Ad hoc Network (MANET) is a collection of wireless mobile nodes communicating with each other while forming all together a self-organized and dynamic network without any pre-existing infrastructure, as depicted in Figure 1. Nodes communicate with each other through a Multi-hop technique while each network node should be able to provide retransmission capabilities using radio signals. Thus each of the nodes acts as a router and must participate in routes discovering and maintaining. A mobile ad hoc network may operate autonomously, as it can be connected to the internet or to other fixed networks.

Nodes in ad hoc networks cooperate with each other to enable a source node to reach the desired destination. They communicate directly when they are in the same transmission range by using a single hop wireless technology like for example Bluetooth or 802.11. They can communicate through a sequence of intermediate devices when they aren't directly connected. Generally, when all network devices are mobile, these networks are frequently referred to as Mobile Ad hoc Networks (MANETs). Nodes mobility causes routes changes and so the network topology is random and dynamic, where all nodes should adapt to changes.

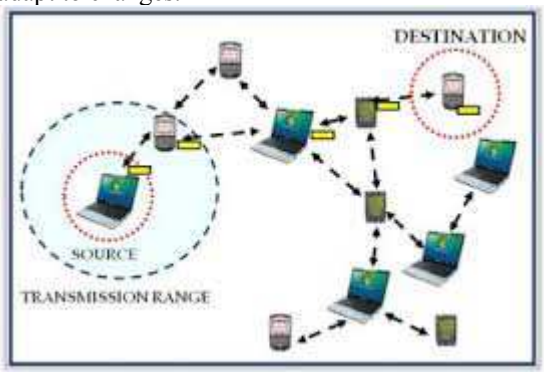

Figure 1: Topology description of MANET Networks

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1.2 Intrusion Detection Systems

Kim [1] has defined the intrusion detection system (IDS) as an automated system whose role is to detect intrusion into a computer system while examining security audits provided by the operating system or monitoring tools network. Its main purpose is to detect unauthorized use, misuse and abuse in a computer system by internal and external users. If unusual activity is detected then the IDS generates an alert to notify the security administrator or else initiate actively a proper response.

Security of MANET can be attempted using two different approaches. Proactive approaches can be used like signature based methods in order to secure the bootstrapping stage or else anomaly detection methods can be implemented. Signature based methods use pre-identified signatures to identify a specific attack while anomaly detection methods intent to identify and observe misbehaviors. In terms of advantages of such method, we can judge that signature based methods allow having low false positive detection rates while anomaly detection methods allow the detection of unknown attacks. Otherwise, signature based methods suffer from higher false negatives which affects precision aspects [2].

Prevention approaches such as authentication and cryptography are also knows as anticipation methods [3, 4, 5, 6]. They were first proposed and implemented in various techniques. However, these applications are not sufficient. If preventive methods are not able to play its role of avoiding the intrusion as a first barrier, and if there is a chance to detect the attack once the intruder succeeds to get inside the network, we still can block the attack from causing any damage to the network. In case of MANET or even 6loWPAN networks, the system becomes more complex which leads to more weaknesses and security problems if using only prevention methods. Here is where the intrusion detection system comes in as a second line of defense [7, 8, 9, 10, 11, 12].

IDSs implemented in MANET are mostly structured in a distributed and cooperative architecture due to mobility of nodes. They are in most cases host based IDS rather than having a network based one. Bio-Inspired techniques are known to be a modern approach to deal with anomaly detection issues. They provide more adaptive solutions to anomaly detection while being effectively distributed, cooperative and lightweight. The wide use of bio-inspired techniques is based on the discrimination between self and non-self with some learning capabilities inspired by various immune algorithms. These concepts of adaptive, lightweight and distributed nature allow bio-inspired methods to be at the top of interest to be used in ad-hoc networks.

2. HUMAN IMMUNE SYSTEM (HIS)

Recent researches have shown an increasing interest in the use of human immune system as a source of inspiration to solve complex problems. The Human immune system benefits from powerful information processing capabilities including models identification, learning, and memorization. It is also known to be a cooperative, distributed, and auto-organizational system. For these reasons, HIS has attracted significant interest to be used as an inspiration metaphor especially in the field of defense and security of information technology (IT) systems. This research field is known as artificial immune systems.

2.1 Definition

The immune system is the best defense mechanism that protects the human body against invading pathogens. It is responsible to keep the human body healthy and to prevent infections. This system is made up of a collection of cells, tissues, and organs that work in collaboration with each other. It identifies and fights potential threats like viruses, bacteria and other organisms that invade the body and cause dysfunctions and diseases. The immune system reacts through a series of steps called immune response while being able to distinguish infectious and foreign pathogens from the body's own tissue [13].

2.2 Physiology

The Lymphatic system consists of various lymphoid organs as bone marrow, spleen, thymus and lymph nodes. The generation process of immune cells is ensured mainly by two organs that are bone marrow and thymus as illustrated in figure2. Bone marrow is the production site of all blood cells and it is the place where certain classes of cells get developed [13]. The thymus is the organ where another class of immune cells migrates in order to pass the maturation stage. The immune system has other types of immune cells, but in this section we will mainly focus on lymphocytes, also named leukocytes and are mainly located at lymph nodes and spleen. Lymphocytes are white blood cells produced in the bone marrow and are responsible for the identification of pathogens. These lymphocytes have receptors located on their surface responsible for antigenic pattern recognition. There are two types of lymphocytes: B cells and T cells. B cells are lymphocytes that

Journal of Theoretical and Applied Information Technology
10th June 2016. Vol.88. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

develop inside the bone marrow. T cells are those lymphocytes that migrate and grow inside the thymus.

Immune cells either circulate throughout the body or reside in a particular tissue like in the spleen or in lymph nodes. Each cell type plays a specific role and cooperates with other cells along processing stages.

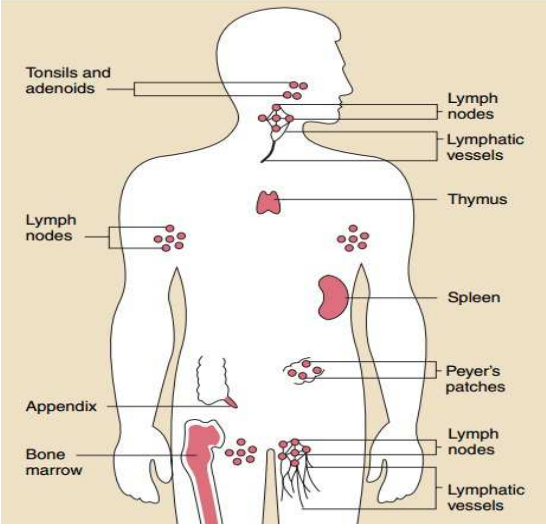

Figure 2: Organs of the immune system

B cells: are immune cells in charge to produce and secrete antibody molecules whenever there is presence of a non self element or a foreign body [13]. Every B cell produces a specific antibody as shown in figure3 (a). Antibodies, also named B Cells Receptors (BCR), are specific proteins that recognize and bind with other particular protein.

T Cells: can be classified into two types: T helper and T killer. T helpers provide essential regulation functions such as activation or suppression of some type of immune response, when T killers perform removal of viruses, microbial invaders, and cancer cells. T cells also have receptors on their surface as illustrated in figure3 (b).

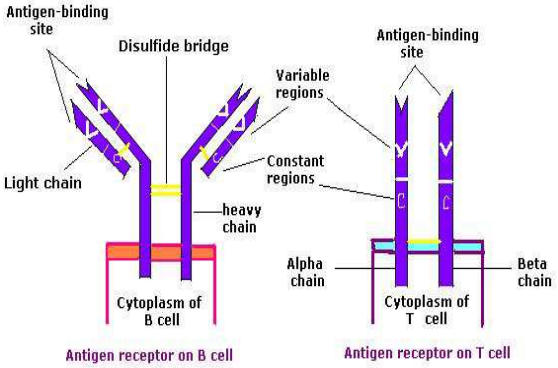

Figure 3: (A) B Cell Receptor (B) T Cell Antigen Receptor

2.3 HIS Protection mechanisms

Our body is protected by a collection of various cells and molecules fighting together against any foreign molecule like bacteria or other invaders. The figure 4 below shows a simplified version of the basic mechanisms of immune defense, which can be summarized by the following steps:

1. When an intruder invades the body, antigen presenting cells (APC) such as macrophages perform the ingestion and digestion of the presented antigen in order to turn it out to fragments of antigenic peptides.
2. These peptides are associated with MHC molecules to enable their connections with T cells that have the ability to recognize the combination of peptide associated with MHC.
3. T cells after being activated by this identification produce and secrete chemical signals named cytokines to mobilize other immune system components.
4. B cells that also have complementary receptor molecules respond to these signals. Unlike T cells receptors, these B cells can recognize the free part of antigens without MHC molecules.
5. After this activation, B cells proliferate and secrete antibody proteins.
6. The connection between antibodies and available antigens lead to the destruction and elimination of these antigens.
7. A number of B and T cells become memory cells having indefinite lifetime, allowing a more adaptable and rapid elimination of the antigen if it runs again in the future.

Journal of Theoretical and Applied Information Technology
10th June 2016. Vol.88. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

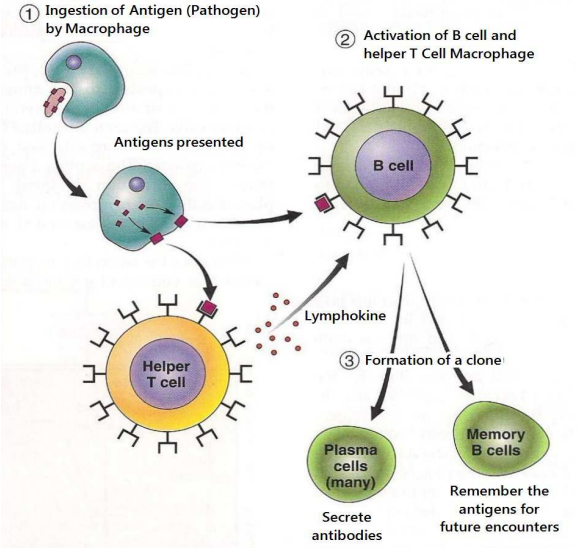

Figure 4: Immune Defense Basic Processes [14]

3. ARTIFICIAL IMMUNE SYSTEM (AIS)

HIS is an ideal protection that protects the human body from various foreign pathogens such as viruses and bacteria. It is able to detect unknown pathogens following a dynamic learning strategy. The fact of applying theoretical immune principals as intrusion detection systems to secure computer networks has gained wide distribution during lasts years under a research field called Artificial Immune System (AIS)[15]. Different models have been developed emulating different aspects of the human immune system. Application areas of AIS have covered multiple domains such as fraud detection [16], robotics [17], machine learning [18], and computer security in a large part [19]. This section gives an overview of some AIS models developed to solve intrusion detection problem.

3.1 Negative Selection Algorithm (NSA)

3.1.1 Concept description

NSA is based on the principle idea that only those T cells that aren't willing to attack self cells are allowed to leave the Thymus. These T cells will then be responsible of identifying non self cells. The idea of generating such accurate detectors is very interesting especially when AIS is applied to anomaly detection or else to system monitoring applications [20]. The majority of NSA based AIS models are based on a random generation of detectors followed by a training phase where only mature detectors that fail to match all self elements are kept. Then test phase consists on using these mature detectors to discriminate between self and non self elements as described by Forrest [21] and De Castro [22]. Figure 5 illustrates NSA basic stages.

As an application of this model, a system called LISYS (Lightweight Immune SYStem) was developed to detect intrusions on a distributed environment. Williams et al: employed this model to detect computer viruses and network intrusion [30].

J. Kim and P. J. Bentley [23] observed that successful IDS must be distributed, lightweight, and self organized. Data and detectors encoding are mostly restricted to binary representation or else real valued vector representation, but comparing methods to rise up matching between detectors and input data can be done using various affinity measures, like landscape affinity [24], r-chunk method [25], Hamming distance [26], r-contiguous bit rule [21], and so forth. These affinity computational methods between binary strings lead to a weakness in terms of covering the problem space [27].

Diverse variations of the algorithm have been proposed [28][29], but they all still use the main characteristics firstly proposed by Forrest [21], including random generation of the detectors set before filtering each detector to keep only mature detectors. A matching threshold is also considered as an approximation to model and judge if there is presence of a matching or not. These variations may differ when developing alternative solutions as divers' detectors generation schemes to improve the algorithm's performance.

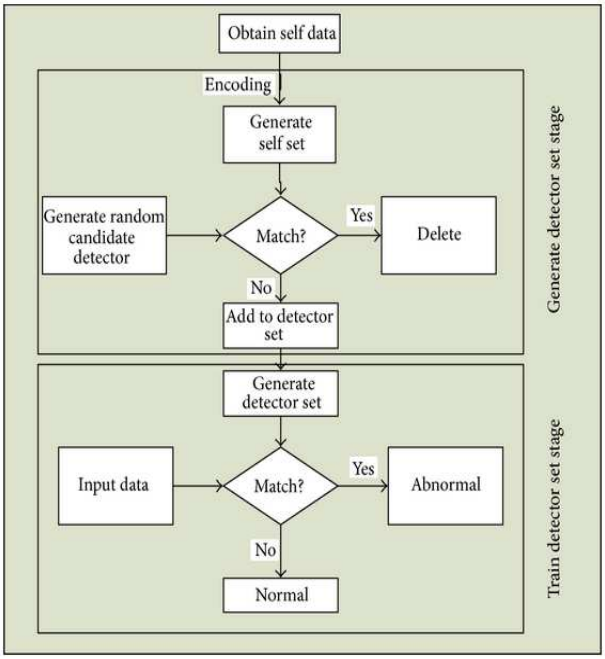

Figure 5: Negative Selection Algorithm [22]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.1.2 Pseudo code of the NSA algorithm

To summarize the algorithm, De Castro[31] have proposed the following pseudo code that starts with the generation of a set of random detectors, then these detectors get filtered to a set of real detectors by keeping only detectors those fail to match any self element. The monitoring stage consists of checking samples individually from the set of introduced antigens against the set of real detectors in order to classify if the sample is "normal" or "anormal".

Input: *S*: Self data labeled "normal", *l:* length of detectors, *r:* matching threshold;
Output: *D*: detectors set;
Begin
While (StopCondition*()***)**
– Generate a set of random detectors (*RD*)
RD GenerateRandomDetectors(*n,l*);
– Filtration of the RD to D by keeping only detectors those fail to match any element in *S*;
For (d in RD)
If (! Matches (d, *S, r*))
d belongs to *D*;
End
– Introduce a set of antigens to be monitored *A;*
A GenerateRandomAntigens(*l*);
– Monitor new sample from the set of introduced antigens by continually checking against the detectors in *D* ;
For (*a* in *A*)
If (! Matches (*a, D, r*)) **Then**
-Classify a as "normal";
Else
-Classify a as "abnormal";
End
End
Return (*D***);**

3.2 Clonal Selection Algorithm (CS)

3.2.1 Clonal selection principle

The immune response could be categorized into primary response and secondary response. The primary response is caused by stimulating activated lymphocytes and may take several weeks to eliminate foreign pathogens. The secondary response, on the other hand, is much faster than the primary response, due to the interesting role that plays memory cells since they can recognize and fight easily against already encountered pathogens. When there is a strong matching between an antibody and an antigen, the corresponding B-cell is then activated to produce clones of itself called memory cells.

Clonal Selection Theory states that memory cells are lymphocyte cells originated due to a Clonal expansion when original lymphocyte proliferate if they are activated by binding to a specific antigen. However, the main features of the clonal selection theory can be summarized as following:

- The cells newly proliferated are similar to their parents, but they get a somatic hypermutation which results in a diversity of antibodies with some random changes;
- Any differentiated clone that is able to carry self-reactive receptors gets eliminated;
- Clonal expansion and differentiation when mature B cells bind with the antigen receptor, this proliferation is proportional to the affinity of the antigen that binds it, the selection of clones guarantee that only clones with higher affinity with the encountered antigen can survive.

3.2.2 Pseudo code of Clonal Selection algorithm

Clonal selection algorithm was initially introduced by De Castro [32] and formally described in [33]. The general algorithm and the most popular and widely used one is called CLONALG. It have been used for multi-modal optimization functions and to perform pattern matching tasks. A pseudo code of this algorithm is outlined below.

Input: *A*: Set of Antigens to be recognized, *n:* number of elements to be removed, *l:* length of detectors, *r:* matching threshold ;
Output: *M*: Memory detectors set;
Begin
While (*StopCondition()***)**
– Generate a set of random detectors (*D*)
D GenerateRandomDetectors(*l*);
For (each *a* in *A*)
– Calculate Affinity with each antibody or detector in *D*;
AF Affinity (*a*, *D*)
– Generate clones of a subset of Detectors in *D* with highest affinity;
*d** Clone(*d in D, with AF>r*) //the number of clones is proportional to its affinity
– Mutation of clones
*d** Mutate(*d* in D*)
– Place a copy of elements with highest affinity to the set of Detector *D* into the Memory set *M*;
M MemoryDetectors(*d* and *d*, AF++* to *D)*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

– Relace n lowest affinity detectors in D with new randomly generated detectors
D ReplaceLowestAffinity*(n,d in D with AF--)*
End
End
Return (*M***);**

3.3 The Danger Theory Model

3.1.1 Mechanism description

Recently, a new theory called the danger theory which has gained much popularity in biological research field. This theory was first proposed by Matzinger in 1994 [34, 35, 36]. It states that the immune response is triggered by the existence of danger and not only following the existence of a foreign element. Hence, the immune system does not react against self elements unless it is dangerous, as it does react against non-self elements unless it is harmless. It is not enough then to detect foreign cells, but it is more important to sense if there is a danger or not based on a correlation between presented alarm signals [37, 39].

In this theory, Antigen Presenting Cells (APC) gets activated through danger alarms. Alarm signals are sent out by distressed cells when they undergo non programmed death caused by a pathogenic attack. These APC cells are called dendritic cells, ones activated, they provide the necessary co-stimulation signals to stimulate T-cells to start an adaptive immune response. Figure 6 illustrates how an immune response can be established according to the Danger Theory. The danger signal establishes basically a danger zone where only B cells that can match antigens inside the danger zone are stimulated to undergo the proliferation process. Other B cells that are far away from the danger zone do not get stimulated.
Dendritic cells can be immature, semi-mature or mature. When immature, dendritic cells collect antigens with both safe and danger signals (such as $PAMP_S$ and inflammatory cytokines) from the local environment. It should then be able to process these input signals to decide about the context information either it is safe or dangerous. If the context is safe then dendritic cell becomes semi-mature, but if the context is dangerous then it becomes mature and initiates an adaptive immune response.

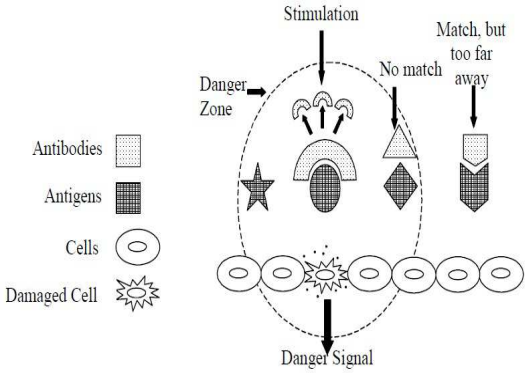

Figure6: The Danger Theory Model [38]

3.1.2 Dendritic cell Algorithm.

The Dendritic Cell Algorithm (DCA) as proposed by Greensmith [40] is a new addition to the field of bio-inspired immunology that introduces the notion of danger, safe and PAMP signals. These captured signals are used to determine the context of presented data. The context is calculated by integrating input signals when simulating the role of dendritic cells. A pseudo code of the algorithm is outlined below.

Inputs: *S*: Set of data items to be classified as safe or dangerous (Antigens with input signals).
Outputs: *DI*: Data items classified or labeled as safe or dangerous + *MCAV*.
Begin
– Create an initial population of dendritic cells (DCs), DC
– Create a set to contain migrated DCs, M
For *each data item* in *S*
– Randomly select a pool *P* of (DCs) from DC population;
For *each DC selected from P* **Do**
– Get the antigen;
– Store the antigen (Add data item to DCs collected list);
– Get the signals and update danger, PAMP and safe signal concentrations;
– Calculate concentrations of cumulative output signals;
If *cumulative Csm > migration threshold* **Then**
– Remove the DC from initial population;
– Migrate DC (Add DC to *M*)
– Create a new and naïve DC;
Else
– DC back to population;
End
End
End

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

For *each DC from M* **Do**
– Assign the cell-context to DC;
If *concentration of Semi<= concentration of Mat* **Then**
Cell context=mature; // context = 1;
Else
Cell context=semi;// context = 0
End
End

For *each data item* in *S* **Do**
– Calculate the number of times this item is presented by a mature DC and a semi-mature DC;
If *nb-semi-mature DC > nb*-mature *DC*
Then
Antigen = normal; //MCAV = 0
Else
Antigen = abnormal; //MCAV = 1;
End
Add data item to labeled or classified data items *DI*
End
End

4. PROPOSITION OF A COMBINED IMMUNE THEORIES ALGORITHM "CITA"

4.1 Inspiration

HIS is the best protection that protects the human body against various types of attacks and virus intrusions; this protection is granted thanks to intervention and cooperation between several immune cells. Of course all these cited immune theories are jointly involved. To best simulate the HIS protection mechanism in order to apply it in the field of MANET security as an intrusion detection system, an approach based on the combination of three immune theories is proposed [41]. The involved immune algorithms are, Dendritic Cell Algorithm (DCA), Clonal Selection (CS), and Negative Selection Algorithm (NSA).

The proposed Algorithm named Combined Immune Theories Algorithm "CITA". This algorithm starts by revealing the context information if it is safe of dangerous using a lightweight version of the Dendritic Cell Algorithm. Similarly as in the human immune system, Dendritic cells are the first cells responsible for digestion of intruder in order to present fragments of the pathogen "antigen" to T and B cells. These lasts then migrate to the site of infection to ensure the elimination of intruders. Dendritic cells and other immune cells work closely. The presented Algorithm also implements both Dendritic cells and other detector called adjacent detectors that are of three types: Immature detectors (ID), Mature detectors (MTD), and Memory detectors (MMD). Each generated Dendritic cell is associated to a set of adjacent detectors combined of ID, MTD and MMD as shown in figure 7.

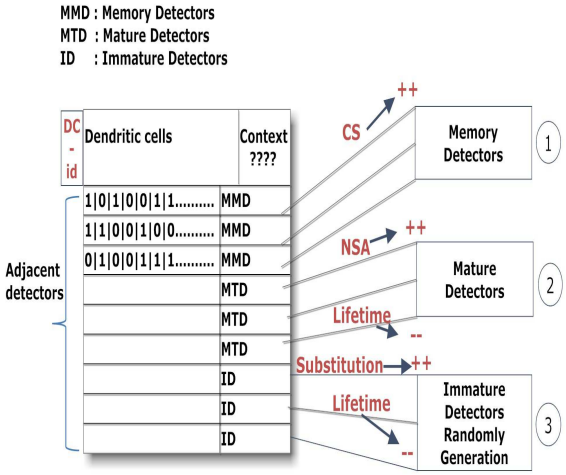

Figure 7: Dendritic Cell And Generation Of Adjacent Detectors From Detectors Population (ID, MTD and MMD)

4.2 Alarm signals & context information

HIS reacts if there is presence of danger and not only following the detection of a foreign element. This is due to the role of some chemical secretions of dead cells called alarm signals. We can differentiate between two types of signals that are apoptosis and necrosis. Apoptosis is the signal received by Dendritic cells when cells undergo a normal programmed death. Necrosis is the signal received when cells undergo accidental cell death. This accidental death occurs during injury tissue and causes inflammation in this last. Similarly, the algorithm triggers two different reactions according to the context information. A lightweight version of DCA is used only to extract this context but not to process the detection. According to the context of each Dendritic cell, the detection will then be ensured by adjacent detectors that will act in different manner and different order.

4.3 The detection process of CITA

Combined Immune Theories Algorithm (CITA) is an algorithm that combines basic principles of multiple immune theories such as DCA, CS and NSA. It uses first DCA principles in order to extract context information only. According to the context, the detection process takes different routes as shown in figure 8.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

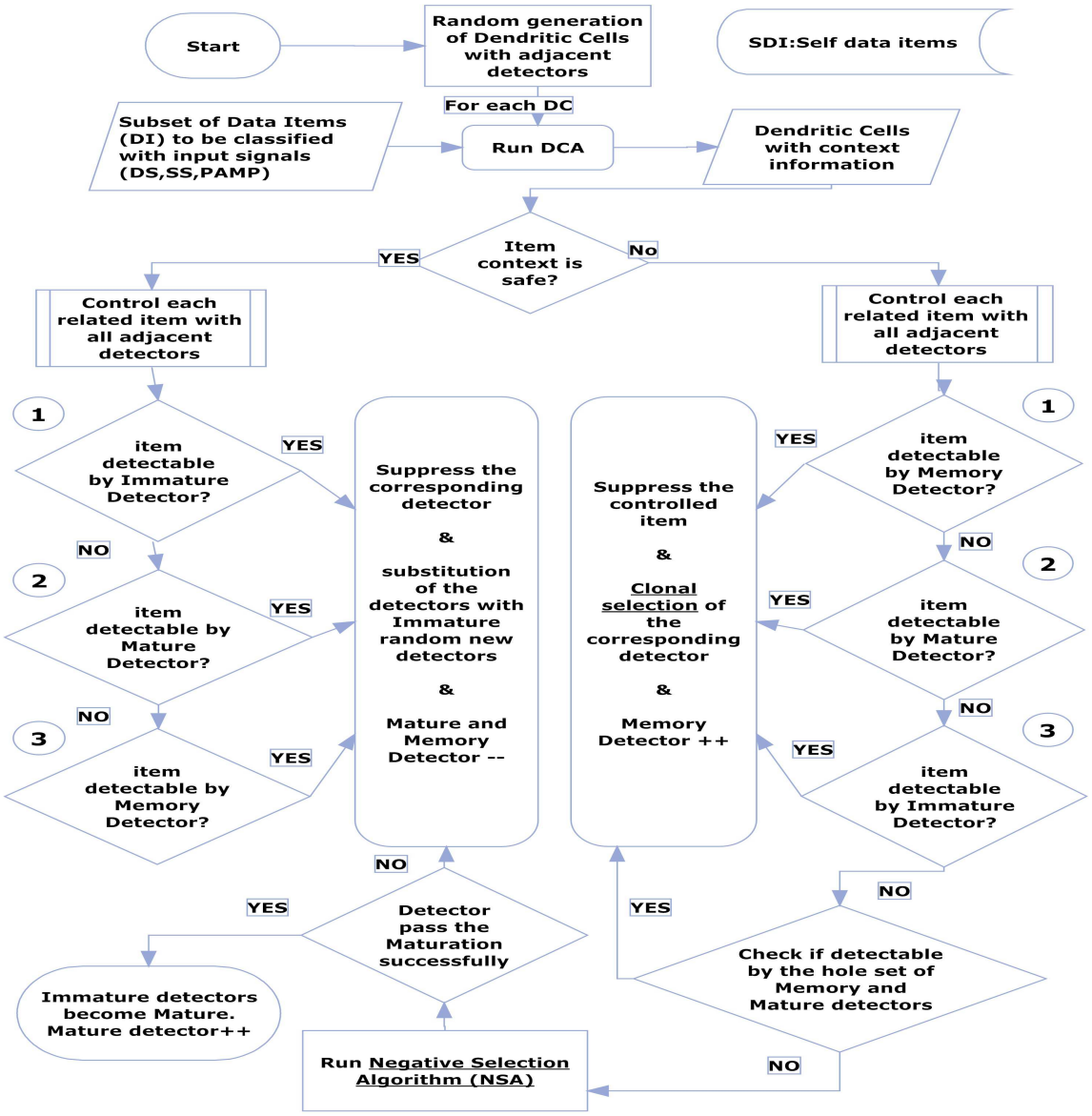

Figure 8: Cita Algorithm Describing The Detection Process While Combined Dca, Cs And Nsa

If context is safe, the algorithm then looks for False Positive (FP) detections in order to suppress the corresponding detectors and replace them by new generated ones. A Dendritic cell is associated to a subset of elements to be classified as shown in figure 9. On the basis of this subset of elements, the related Dendritic cell runs DCA. Subset elements are nothing other than all neighbor nodes in the reality. These elements are mostly responsible of the maturation of the related Dendritic cell since they are source of input signals. The detection process starts in this case by controlling each item that belongs to the subset of elements using adjacent Immature Detectors (ID) in first stage then adjacent MD and finally adjacent MMD. This part of the algorithm allows finding out detectors that causes false positive detections in order to suppress them and consequently reduce false positive rates.

This is the case when adjacent cells can get replaced (ID--, MTD--, MMD--). Cells get substituted also when lifetime is expired. The chosen order of adjacent detectors involved helps reducing the algorithm complexity since it allows a brief get out from the loop.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

If context is dangerous, the order of adjacent detectors implicated is inversed. This is in order to reduce the algorithm's complexity and to have a quick response. This metaphor is inspired by the adaptive immune response. Mostly, the response here is specific since introduced antigen is already known. Specific memory cells then first interact and take control to eliminate the intruder immediately. This part of the algorithm helps increase True Positive (TP) detections. Elements of the subset related to the matured Dendritic cell get controlled first by adjacent MMD; then by adjacent MTD; later by adjacent ID and finally by the hole set of Mature and Memory detectors even from other Dendritic cells adjacent detectors. Whenever detection is in place, the detected element gets removed. The corresponding detector undergoes Clonal Selection (CS) to allow evolution of detectors population and to keep and increase corresponding Memory detectors MMD++. In case where no one of the detectors gets to catch up the intrusion, then related ID gets substituted by new ones. New generated detectors then pass the Negative selection algorithm NSA with self data items to become MTD and to reenter the detection process.

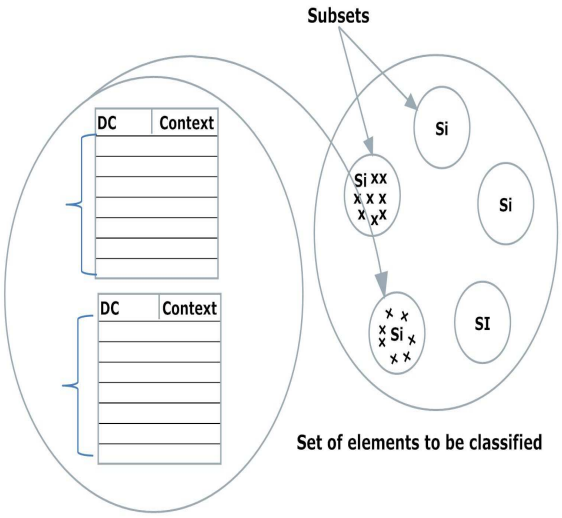

Figure 9: Association Between Each Subset Of Data Items To Be Classified And Dendritic Cells

4.3 Adjacent detectors life cycle

The detectors population follows an evolutionary mode since the system cannot generate detectors infinitely. Detectors that will end up their lifetime should be substituted by new generated detectors as proposed by Hofmeyr[42]. Detectors then get the maturation stage through the Negative selection Algorithm to avoid auto immunity by having detectors that could match to self elements. Clonal selection allows the proliferation of specific detectors that are responsible of a real detection. They could be either Mature or Immature detectors. It allows then detectors to differentiate and to add Memory detectors to the detectors population. Figure 10 shows the detectors lifecycle. All of the three types of Detectors can get suppressed and replaced by new randomly generated detector if they are source of a false positive detection. This happens generally if detection is in place even if context is safe, or else if a detector reaches its lifetime.

Following the described evolutionary mode of detectors generation process, and after running the algorithm a set of times, we can start feeling that the detectors population gets more precise and efficient. Detectors filtering is done by throwing away useless detectors and by replacing them by more mature and memory detectors. The detectors population size is also dynamic since it grows proportionally with the number of detected intruders. The population size then is unpredictable but depends on the state of controlled environment.

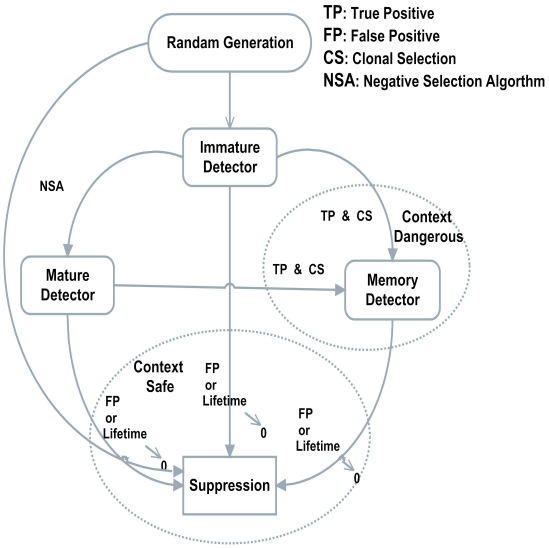

Figure 10: Adjacent Detectors Life Cycle (ID, MTD, MMD)

4.4 Implementation of CITA in MANET

Mobile ad-hoc network is a self-organizing and rapidly deployable network. MANET consists of a mass of wireless nodes that are able to communicate with each other through a multi-hop technique. Nodes must be able to play the role of routers and provide retransmission capabilities if destination nodes are out of range. Communication between nodes can be established without any pre-existing network and using

Journal of Theoretical and Applied Information Technology
10th June 2016. Vol.88. No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

wireless links. Neighbor nodes then exchange valid routes as they can exchange some small amount of data. The implementation of CITA algorithm in Mobile Ad hoc networks is ensured through the following process as described in figure11.

: R Req (Route request)
: Exchange of:
1-Context
2-Updated Self Data Items (SDI)
3-Updated population of detectors
4-Updated malicious nodes_ids

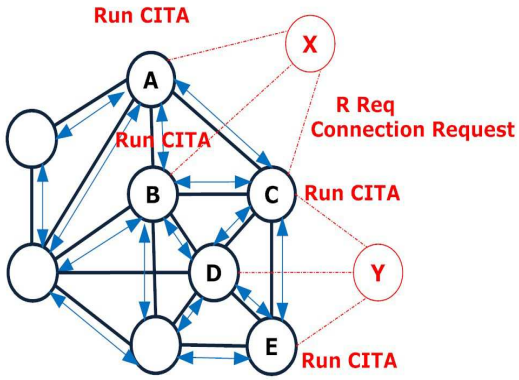

Figure 11: Implementation Of CITA In MANET

Network nodes run CITA following the reception of high rate of RREQ from a neighbor node, or whenever they get asked for a route from a new node that doesn't belong to self data items. They also run CITA whenever context information exchanged from neighbor nodes is changed to dangerous.

Each node keeps a copy of the following data: 1) self data items, 2) detectors population, 3) malicious nodes identifications (Id). Those can be considered in addition to input signals as the input data of CITA whenever is needed to be run on a network node. The output then will be the updated version of detectors population, updated self data items, updated list of malicious nodes id, and the evaluated context. The output data of CITA on a node should be exchanged with neighbor nodes whenever changed after the execution of CITA. Figure12 describes input and output data of CITA.

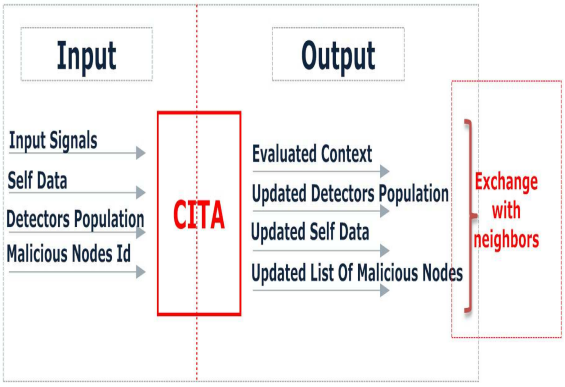

Figure 12: Input and Output of CITA Algorithm

4.5 Implementation of CITA with the AODV Routing Protocol.

CITA is an algorithm that gets triggered on a network node particularly if an alarm signal is sent out by the monitoring system. In the case of Resource Consumption Attack (RCA), alarm signal is sent out whenever high amount of RREQ packets is received. CITA can be implemented with various routing protocols that apply to MANET, whereas it is much more compatible with reactive routing protocols. In this study, CITA is integrated to the AODV routing protocol.

Ad-Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol when routes information is only transmitted by nodes on-demand [43]. AODV is widely used and consists of finding network nodes whenever users intent to send data. The sender floods RREQ so that the destination node or an intermediate node can replies later by sending back an up to date or fresh route between source and destination called Route Reply (RREP). AODV then once received all active routes chooses the shortest path. The source node sets a timer to wait for RREP before it can broadcast again RREQ packet through the network.

Attacker can adopt three different malicious behaviors: They can keep broadcasting the RREQ packets without even waiting for the RREP in order to consume network nodes energy. Power resources are a major issue in MANET since nodes run out of any power supply except batteries limited resources. Attackers also can send back falsified RREP. They can firmly drop packets. Those three misbehaviors are the major issues behind a wide part of MANET attacks.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CITA Algorithm is used to enhance AODV in term of security. It is run following the reception of an alarm signal due to the reception of high rate of RREQ from a single node during a unit of time. CITA is also triggered following the reception of dangerous context exchanged from neighbor nodes. If the sender of RREQ packets is recognized as a malicious node, then all packets that will be originated from this node will be immediately dropped, and the malicious node will be excluded from all valid routes. All paths including the malicious node then will be declared failure links and new routes discovery then will be launched to avoid participation of malicious nodes in active paths. A dangerous context then will be exchanged with neighbors as well as other updated data.

4.6 Initial network configuration and processing.

The network's configuration and processing takes place following the steps described below:

- Network is first configured with a set of trusted nodes called self elements SI.
- Each node has an initial set of detectors related to its own DC.
- New nodes then intent to join the network increasingly. Some of them are safe nodes with no bad behavior, and some of them are malicious nodes that will initiate some network attacks. Both safe and malicious nodes form together the set of data to be classified. In the reality even self data items or self nodes get controlled by neighbor nodes especially if context is dangerous. They can be excluded from the list of self data items if impersonated.
- CITA's objective is to classify the inserted nodes as normal nodes and can add them to the list of self data, or else as malicious nodes and then it should block them.
- CITA is an auto-organized algorithm that follows an evolutionary strategy to filter detectors and replace them by more efficient ones.

4.7 Simulation Results

4.7.1 Simulation Environment

Simulations are conducted using Network Simulator-2 version 2.35[44], it is one of the most popular and free network simulator that support simulating MANET with all the existing protocols already embedded. Most of MANET attacks also can be easily involved. The challenge then was how to find a simple method to implement CITA algorithm within this simulation environment. Two experiments then are adopted for multiple network configurations. The first experiment is done using the secure AODV (SAODV) routing protocol [45], and the second one is conducted using CITA algorithm implemented with AODV. Results then are compared for different network configurations.

The simulation is done using 50 mobile nodes. To each mobile node is associated a unique identifier ID that ranges from 1 to 50. Simulations time is of 900 seconds. The first 100 seconds is reserved to a learning phase where only 20 nodes are involved. This stage is very important since an initial network topology is created, and each node gets to update its local data as Self Data Items that represents the list of the first 20 nodes ID. Each node that run CITA creates a dendritic cell with adjacent detectors. The first detectors population is exchanged with every single node and gets the maturation stage using NSA. Detectors population is also exchanged between network nodes. The following 800 seconds is set to be the detection phase. During this detection stage, mobile nodes keep moving following the Random Way Point (RWP), and after each 45 seconds 2 nodes get inserted into the network. One of the two nodes is normal with no bad behavior, but the second inserted node starts flooding RREQ without even waiting for a RREP. Simulation parameters are shown in table 1:

Table 1: Ns-2 Simulation Parameters

Parameter	Value
Simulation Time	900 s (100s learning + 800s detection phase)
Application traffic	CBR
Simulation Area	1000 X 1000 m
Radio Range	250 m
Number of Nodes	50
Packet Size	128 bytes
Mobility model	Random Way Point (RWP)
Routing Protocol	AODV / CITA with AODV
Transmission rate	2 packets/s
Maximum speed	1 m/s
Available bandwidth	2Mbps
Number of misbehaving nodes snapshot measures	3,6, 9,12,15

CITA Algorithm requires setting up some initial parameters like the number of adjacent detectors and the definition of alarm signals.

The number of adjacent detectors to each dendritic cell is chosen to be 10 detectors

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

initially Immature, then they get the maturation stage through NSA and some of them become Memory detectors if they can get to detect a real intrusion. Each detector is a binary string of 24 bits (3 bytes); however a node ID is codified using only 8 bits. The matching rule between a node ID and a detector is r-contiguous bits with L=8[46]. A detector can match up to 17 nodes by transiting the starting position of the matching rule.

Alarm signals configuration is also required for the DCA part of CITA Algorithm in order to correlate these signals and to extract context information. The definition of these signals is based on the nature of the studied attack. Malicious nodes in this study use Resource Consumption Attack (RCA) since they keep broadcasting RREQ. Alarm signal then is defined as high rate of RREQ packets received by a single node, which indicates strongly the existence of Resource Consumption Attack [47].

4.7.2 Results and discussions

Simulations are conducted using both the proposed CITA algorithm implemented with AODV protocol, and the secure AODV routing protocol. The same network scenario described in section 4.7.1 was run for both experiments in order to compare the performance of CITA Algorithm compared to SAODV, in terms of Detection Rates, False positive rates, Throughput, and Packet Delivery Rates. Each experiment was repeated 5 times and the average is tracked so that results can be more precise. Obtained results are shown consequently in figures 13, figure 14, figure 15 and figure 16.

Figure 13 and Figure 14 represent consequently the detection rate (DR) (also named True positive (TP) detection rates), and False Positive Rate (FPR) for both CITA-AODV and Secure AODV. CITA-AODV shows a relatively higher degree of DR than its analogous, as well as it shows a comparatively lower FPR throughout the experiment time.

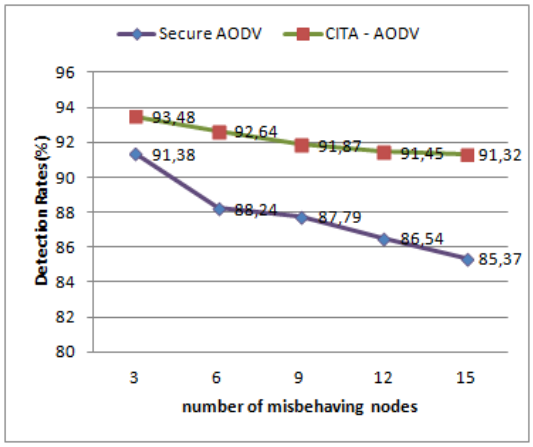

Figure 13: Detection Rates According To The Number Of Misbehaving Node.

From Figure 13, an average of 92.15% of true detections is trucked for CITA-AODV, while Secure AODV records an average of 87.86%. It is an increase of 4.29%. At the beginning or the experimentation when only 3 nodes act as misbehaving nodes, the increase of DR for CITA-AODV is of 2.1%, but when 15 of inserted nodes are misbehaving or malicious, then the increase of DR is of 5.95%. This comparison leads us to judge that in case of CITA AODV, the network gets able to auto learn and react against RCA Attacks after the learning period. This is can be explained by the fact that the detectors population becomes more precise and mature which allow higher detection rates.

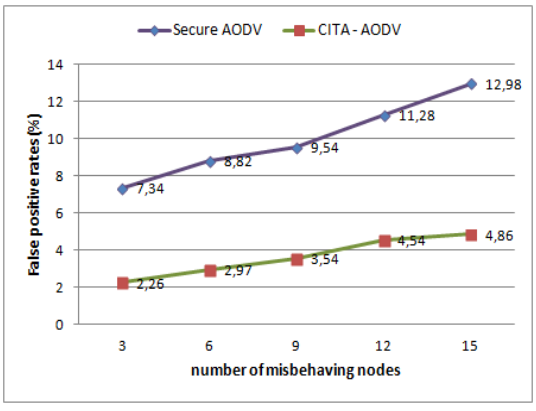

Figure 14: False Positive Detection Rates According To The Number Of Misbehaving Node.

False positive detection rates are also much lower in case of CITA AODV as shown in figure 14, since the difference is of 5.08% at the beginning of the experimentation and goes up to 8.12% in the worst case scenario when 15

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

nodes are malicious. CITA AODV maintains slightly a good precision and persistence in term of FPR even with a growing number of RCA attacks. This is can be explained by the elimination of mismatching detectors in case where context is safe.

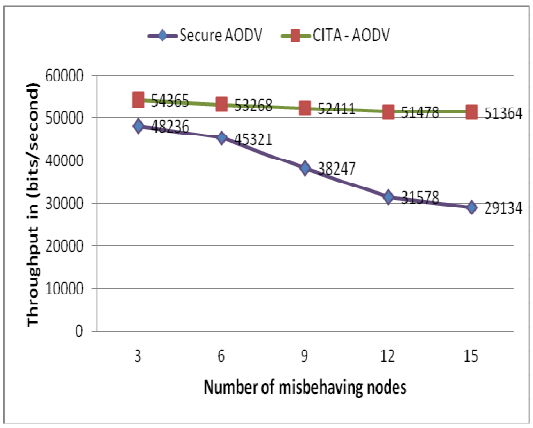

Figure 15: Throughputs according to the number of misbehaving node.

Network throughput is given by the fraction of received bits for all network destination nodes per a period of time. It represents the network's transmission capacity. Network throughput depends on available bandwidth and transmission rate. It is clear from figure 15 that in case of both CITA AODV and Secure AODV, the throughput is influenced by RCA. The increasing number of RREQ flooded in the network leads to congestions which degrades the available transmission channel. CITA AODV performs better throughput levels compared to Secure AODV. The average throughput of CITA is of 52577 bps while an average of 38503 bps is recorded in the case of Secure AODV.

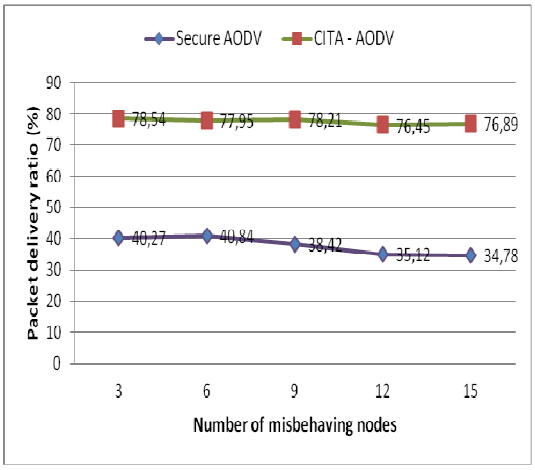

Figure 16: Packet delivery ratio according to the number of misbehaving node.

Packet delivery ratio PDR is another criteria used in MANET to evaluate the performance of a protocol. It gives the ration of the number of delivered data packet to the destination divided per the number of packets sent. From figure 16, CITA AODV maintains a relatively high PDR of 77.6% as an average compared to Secure AODV that registers an average of 37.88%.

It is clear from the simulation results that network performance degrades proportionally with the increasing number of misbehaving nodes for both cases. Except that the CITA-AODV sustains much better resistance compared to secure AODV. CITA-AODV often tends to keep a steady pace after a learning period. It is in fact an auto learning, auto adaptive and evolutionary algorithm. The contribution of this study is then the proposition of an immune inspired intrusion detection system named CITA. This proposed algorithm that is based on the combination of multiple immune theories proves better performance when it is used with the AODV routing protocol (CITA-AODV) compared to SAODV. Security is enhanced since CITA-AODV registers higher detection rates and lower false positive rates compared to SAODV in presence of resource consumption attack. CITA-AODV registers also better performance related to other network parameters such as throughput and PDR.

5. CONCLUSIONS AND PERSPECTIVES

This paper proposes an intrusion detection system that is implemented to enhance MANET security. The proposed IDS is an Algorithm named Combined Immune Theories Algorithm "CITA". As indicated from its name, CITA combine three major immune algorithms that are NSA, CSA, and DCA. This algorithm starts by revealing the context information if it is safe of dangerous using DCA. According to the sensed context, a set of tests, suppressions, cloning, and substitutions are applied to the detectors population to get filtered during a learning phase. Simulation results show better performance of the proposed CITA algorithm embedded with AODV routing protocol in presence of RCA compared to Secure AODV as given in section 4.7.2. Network performance is measured

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

based on DR, FPR, Throughput, and PDR. The objective of the proposed approach is the enhancements of MANET security compared existing protocols such as SAODV protocol. This is hopefully achieved since CITA-AODV registers higher detection rates and lower false positive rates which mean better precision of the proposed IDS. The definition of a standard normal behavior without considering the nature of attack is a challenging task. The monitoring system needs that standard normal behavior in order to report all deviations caused by an attacker, instead of defining an interval of tolerance already defined for each type of attack.

Future work will study the impact of CITA on some other performance parameters such as Control overhead, End to End Delay, Packet Loss, and Mean hop count. Performance analysis of CITA also will be studied in presence of Packet dropping attack.

REFRENCES:

[1] J W Kim. "Integrating Artificial Immune Algorithms for Intrusion Detection", *PhD thesis Report*, University College London, 2002.

[2] Kazemitabar A. "Enhancing Bio-inspired Intrusion Response in Ad-hoc Networks" *Phd thesis Report*, Edinburgh Napier University, August 2013.

[3] M. G. Zapata, "Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing," *ACM Mobile Computing and Communication Review (MC2R),* Vol. 6, No. 3, pp. 106-107, July 2002.

[4] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)*, pp. 3-13, June 2002.

[5] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," *Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02)*, pp. 12-23, September 2002.

[6] A. Perrig, R. Canetti, D. Tygar and D. Song, "The TESLA Broadcast Authentication Protocol," *RSA CryptoBytes*, 5 (summer 2002)

[7] Y. Xiao, X. Shen, and D.-Z. Du (Eds.) "A Survey on Intrusion Detection in Mobile Ad Hoc Networks" *Springer*, pp. 170 - 196 2006.

[8] A. Rghioui, A. Khannous and M. Bouhorma, " 6lo Technology for Smart Cities Development : Security Case Study", *IJCA* , vol 92, No.15, April 2014.

[9] A. Rghioui, S. Bouchkaren and M. Bouhorma, "Symmetric Cryptography key management for 6 LoWPAN networks", *JATIT*, Vol 73, No. 3, March 2015.

[10] A. Rghioui, A. Khannous and M. Bouhorma, "Denial-of-Service attacks on 6LoWPAN-RPL networks: Threats and an intrusion detection system proposition", *Journal of Advanced Computer Science and Technology JACST*, pp 143-153, 2014.

[11] A. Rghioui, A. Khannous and M. Bouhorma, "Monitoring behavior-based Intrusion Detection System for 6loWPAN networks", *International Journal of Innovation and Applied Studies IJIAS*, vol 11, No 4,pp 894-907 , Jun 2015.

[12] A. Rghioui, A. Khannous, S. Bouchkaren and M. Bouhorma, "Security Key Management Model for Low Rate Wireless Personal Area Networks", *International Journal of Computer Science and Security IJCSS,* vol 8, No. 5, 2014.

[13] De Castro .L.N & Von Zuben .F.J "Artificial Immune Systems: Part I - Basic theory and applications", *Technical report*, *TR-DCA-01/99*, December 99.

[14] Suzanne G. "Classification of the Immune System", *https://www.studyblue.com.*

[15] S.X.Wu andW. Banzhaf, "The use of computational intelligence in intrusion detection systems: a review," *Applied Soft Computing Journal*, vol. 10, no. 1, pp. 1–35, 2010.

[16] M. F. A. Gadi, X.Wang, and A. P. do Lago, "Credit card fraud detection with artificial immune system," *Computer Science*, pp. 119–131, Springer, Berlin, Germany, 2008.

[17] J. Timmis, A. Tyrrell, M. Mokhtar, A. Ismail, N. Owens, and R. Bi, "An artificial immune system for robot organisms," in Symbiotic Multi-Robot Organisms: Reliability, Adaptability, Evolution, pp. 268–288, *Springer, Berlin*, Germany, 2010.

[18] A. Watkins, J. Timmis, and L. Boggess, "Artificial immune recognition system (AIRS): an immune-inspired supervised learning algorithm," *Genetic Programming and Evolvable Machines*, vol. 5, no. 3, pp. 291–317, 2004.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[19] L. N. de Castro and J. Timmis. "Artificial Immune Systems: A New Computational Intelligence Approach". *Springer, Berlin*, Germany, 2002.

[20] L.N De Castro, J I Timmis, "Artificial immune system as a Novel Soft Computing paradigm", *Soft Computing Journal* , Vol 7 July Computing laboratory, University of Kent at Canterbury , 2003

[21] S. Forrest, L. Allen, A. S. Perelson, and R. Cherukuri, "Selfnonself discrimination in a computer," in Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 202–212, Oakland, Calif, USA, May 1994.

[22] L.N CASTRO, F. J VON ZUBEN, "Artificial immune system: Part II- A survey of applications", Technical Report, DCA-RT, Feb 2000

[23] Kim, J., Bently, P.J. "An Evaluation of Negative Selection in an Artificial Immune System for Network Intrusion Detection". In Proceedings of the Genetic and Evolutionary Computation conference, 2001.

[24] P. K.Harmer, P. D. Williams, G. H. Gunsch, and G. B. Lamont, "An artificial immune systemarchitecture for computer security applications," IEEE Transactions on Evolutionary Computation, vol. 6, no. 3, pp. 252–280, 2002.

[25] J. Balthrop, F. Esponda, S. Forrest, andM. Glickman, "Coverage and generalization in an artificial immune system," in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO '02), pp. 3–10, July 2002.

[26] S. Forrest and S. Hofmeyr, "Immunity by design: an artificial immune system," in Proceedings of the Genetic and Evolutionary Computation Conference (GECCO '99), pp. 1289–1296,Morgan-Kaufmann, San Francisco, Calif, USA, 1999.

[27] F. Gonzalez, D. Dasgupta, and J. Gomez, "The effect of binary matching rules in negative selection," in Genetic and Evolutionary Computation-GECCO 2003, vol. 2723 of Lecture Notes in Computer Science, pp. 195–206, Springer, Berlin, Germany, 2003.

[28] Z. Ji and D. Dasgupta, "Revisiting Negative Selection Algorithms". Evolutionary Computation, vol. 15, pp. 223-251, 2007.

[29] D. Dasgupta, S. Yu, F. Nino "Recent Advances in ArtificialImmune Systems: Models and Applications", Applied Soft Computing Journal, 2010.

[30] P. K. Harmer. "A distributed agent architecture of a computer virus immune system". Master's thesis, Air Force Institute of Technology, Air University, March 2000.

[31] L.N. DE CASTRO, F. J. VON ZUBEN. "The Construction of a Boolean Competitive Neural Network Using Ideas from Immunology". Neurocomputing, 50C, pp. 51-85, 2003.

[32] L. N. D. Castro and F. J. V. Zuben, "The Clonal Selection Algorithm with Engineering Applications" *Genetic and Evolutionary Computation Conference (GECCO'00) - Workshop Proceedings*, Las Vegas, Nevada, USA, 2000.

[33] L. N. d. Castro and F. J. V. Zuben, "Learning and optimization using the Clonal selection principle" *IEEE Transactions on Evolutionary Computation*, vol. 6, pp. 239-251, 2002

[34] Matzinger. P "Tolerance, danger and the extended family", *Annual reviews in Immunology*, 12: 991- 1045, 1994.

[35] P. Matzinger. "An innate sense of danger". *Seminars in Immunology*, 10:399-415, 1998.

[36] Matzinger. P "The Danger Model: A renewed Sense of Self", Science 296: 301-305,2002.

[37] U Aickelin, P Bentley, S Cayzer, J Kim, J McLeod, "Danger Theory: The Link between AIS and IDS?" *Proceedings ICARIS-2003, 2nd International Conference on Artificial Immune Systems*, pp 147-155, 2003

[38] U. Aickelin and S. Cayzer "The Danger Theory and Its Application to Artificial Immune Systems" *Proceedings of the 1st Internat Conference on ARtificial Immune Systems (ICARIS-2002)*, pp 141-148, Canterbury, UK, 2002

[39] Aickelin. U & Bentley . P & Cayzer. S & Kim . J & McLeod. J « Danger Theory: The Link between AIS and IDS? », *in Proceedings of the second International Conference on Artificial Immune Systems (ICARIS-03)*, 147 – 155, 2003.

[40] Greensmith. J & Aickelin. U & Cayzer. S "Introducing Dendritic Cells as a Novel Immune-Inspired Algorithm for Anomaly Detection", *Proceeding (ICARIS-05),* 2005.

[41] A. Khannous and F. Elouaai, "A new approach to artificial immune system for intrusion detection of the mobile ad hoc networks", *IJCA journa,l Vol 92, No.15, pp April 2014*

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[42] S. A. Hofmeyr and S. Forrest, "An Immunological Model of Distributed Detection and Its Application to Computer Security", The University of New Mexico, Albuquerque, NM, USA, 1999.

[43] Gupta, A., Sadawarti, H., & Verma, A. "Performance analysis of AODV, DSR & TORA routing protocols." *IACSIT international journal of Engineering and Technology* (2010) pp.226-231.

[44] Network Simulator-2 tutorial web site, at: www.isi.edu/nsnam/ns/tutorial.

[45] D. Cerri and A. Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", *In Communications Magazine, IEEE, Vol. 46*, No. 2. pp. 120-125, February 2008

[46] Detours, V., Sulzer, B. & Perelson, A. S. (1996), "Size and Connectivity of the Idiotypic Network are Independent of the Discreteness of the Affinity Distribution", J. theor. Biol., 183, pp. 409-416.

[47] Abdelhaq, M., Hassan, R., Ismail, M., Alsaqour, R. and Israf, D. (2011) "Detecting Sleep Deprivation Attack over MANET Using a Danger Theory-Based Algorithm". *IJNCAA,* 1, pp 534-541.