International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.211-228
http://dx.doi.org/10.14257/ijsia.2016.10.9.21

MANET: Securing AODV Based on a Combined Immune Theories Algorithm (CITA)

Anass Khannous[1], Fatiha Elouaai[1], Anass Rghioui[1] and Mohammed Bouhorma[1]

[1]*LIST, Faculty of Science and Technology of Tangier, Abdelmalek Essaadi University, Morocco*
[1]*khannous@ensat.ac.ma*

Abstract

Mobile Ad hoc Networks consist of a set of mobile nodes communicating with each other in a decentralized and dynamic topology where nodes provide retransmission capabilities. Communications between source nodes and destinations go through routes represented by a set of intermediate nodes that are required to adapt and behave in response to some actions according to orders given by the chosen routing protocol. Absence of a centralized architecture, in addition to open wireless medium of Ad hoc networks, as well as nodes mobility are ones of the network characteristics that render the environment much vulnerable to different routing attacks. A wide range of current researches focus on enhancing MANET security using various techniques like cryptography, but these mechanisms creates too much overhead. Artificial Immune Systems provide intrusion detection techniques based on the abstraction of the human immune system. They are known to be very efficient and lightweight algorithms. Multiple immune theories are implemented like Negative selection, Clonal selection, Danger theory, Immune network...etc. This paper proposes the use of combined immune theories as an Intrusion Detection System that integrates to the AODV routing protocol and that can sense the presence of non-trusted nodes, as it can eliminate them from the network. The proposed approach is tested and validated in presence of Packet Dropping Attack. Promising results in terms of network performance then are discussed.

Keywords*: MANET, Security, Combined Immune Theories Algorithm, CITA, Artificial Immune system, AODV, routing attacks*

1. Introduction

Mobile Ad hoc networks (MANETs) are rapid deployable networks that don't require any pre-existing infrastructure and can be used in a decentralized manner where nodes can act as routers. These properties increase the feasibility of the above networks to be applied in war-torn regions and earthquake-prone areas.

MANET security is an attractive field that draws attention and motivation of researchers for many reasons. Ad hoc networks are vulnerable to different types of attacks due to some intrinsic properties such as the limitation of energy and bandwidth, as well as the lack of a fixed infrastructure that makes the use of traditional techniques applied in wired networks rather complicated. Such networks are considered to have dynamic and rapidly changing topology. Thus, lightweight computing techniques are most envisaged to secure MANET.

Routing attacks are highly diversified and influence almost all existing routing protocols. A large number of intrusion detection systems (IDSs) have been proposed to better secure routing protocols in MANETs [1]. Some of the proposed IDSs are based on cryptographic techniques but in most cases they show some weaknesses especially

ISSN: 1738-9976 IJSIA

in terms of the increased control overhead that can be explained by the transmission of extra security data within routing packets such as digital signatures and hash functions.

A new trend of intrusion detection systems intend to simulate and abstract the role of the human immune system (HIS) to protect the human body and apply it in the security field what's known as Artificial Immune Systems (AIS). The analogy between HIS and MANET environment is based on many similarities that exist between these independent systems in terms of the functioning mechanism as concluded from the study in [2]. HIS protects the body from a large number of pathogenic intrusions, viruses and harmful bacteria even without any prior knowledge about the structure of these intruders. This robust defense granted by HIS is expected to be transmitted into artificial immune systems in order to protect and enhance the security of ad hoc networks. AISs then are defined as the abstraction of one or more HIS concept or immune theories and their replication as a set of computational and immune algorithms. AIS security techniques are judged to be more compatible with MANET where no central management points are present. Those techniques are also known to be less complex and more adaptable since they take up the challenges and limitations of such networks.

This paper gives an overview of some researches that implement major immune algorithms such as the Negative selection Algorithm (NSA), the Clonal Selection (CS) and Dendritic Cell Algorithm (DCA) in order to propose an algorithm called "Combined Immune Theories Algorithm – CITA" that combines these three immune algorithms as well as some other immune principals. CITA is then integrated to the AODV routing protocol (CITA-AODV). The objective is to investigate the capability of the proposed approach to detect packet drop attacks and to keep better network performance even when faced by this kind of attack. Network simulator 2 (NS2) is used as the simulation tool that allows us to evaluate the network performance based on the calculation of some key parameters such as true positive detection rate (TP), false positives (FP), Throughput, End to end delay, Packet Delivery Ratio (PDR),and Routing overhead. Obtained results are discussed and compared with the secure AODV that uses some cryptographic techniques.

2. Protection Mechanism of the Human Immune System

Human body is protected by a collection of various cells and molecules fighting together against any foreign molecule like bacteria or other invaders. Figure 1 below shows a simplified version of the basic mechanisms of immune defense [3], which can be summarized by the following steps:

1. When an intruder invades the body, antigen presenting cells (APC1) 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.

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.

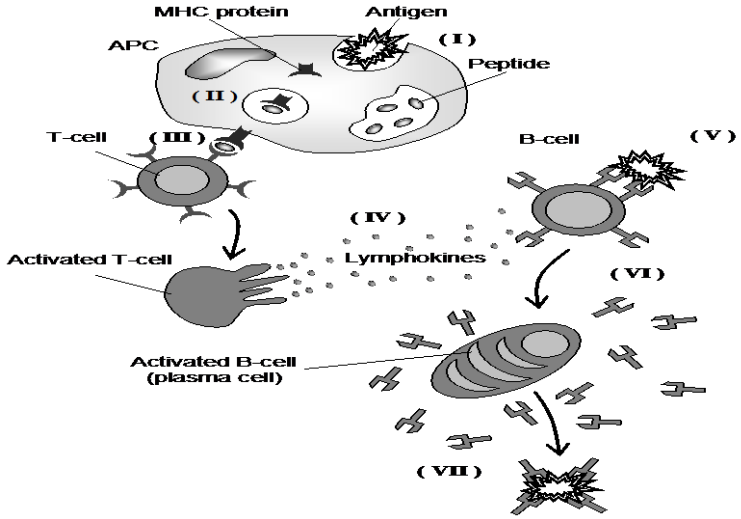
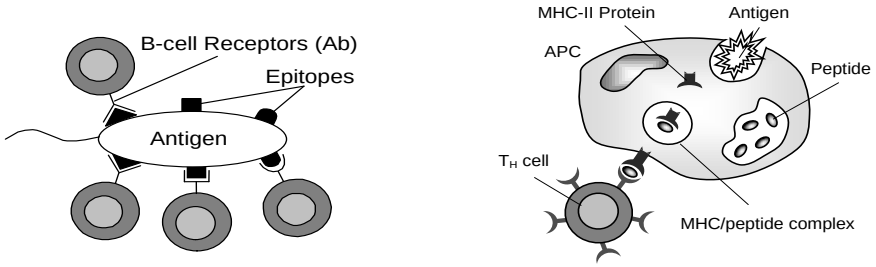


Figure 1. The Immune Defense Basic Process [3]

Identification and activation are two basic processes of the human immune system:

2.1. Identification Process

The recognition of an antigen is ensured by specific lymphocytes that are present in the tissue and are ready to react following the presence of corresponding antigens. Indeed, each immune cell (either B or T cell) has a set of specific receptors on its surface and these receptors have a complementary shape to determinant substances present on the antigens surface known as epitopes. An epitope, also known as antigenic determinant, is the part of an antigen that is recognized by the immune system. Antigen is identified whenever there is a matching between an immune cell's receptor and the epitope of the antigen. B and T cells have a similar structure but they have a different recognition mechanism. As a matter of fact, B cells are able to recognize free antigens as shown in Figure 2 (a), while T cells have the ability to recognize antigen that is presented by MHC3 molecules as illustrated in Figure 2 (b).



(a) (b)

Figure 2. Identification Mechanism of B and T Cells [3]

2.2. Activation Process of HIS

The identification of the antigen is the first step to generate an immune response to destroy the recognized antigen. Then, the human immune system uses approximate

matching to trigger the immune response, and the pairing between a lymphocyte receptor and an epitope of a particular antigen is determined according to the affinity between this lymphocyte cell and the antigen [3]. If the match between a cell receptor and an epitope is strong then affinity is high; otherwise, it is a low affinity. Antibodies secreted by mature B cell are activated directly or indirectly, the activation mode being determined according to an affinity threshold. When a B cell matches an antigen with a higher affinity than the affinity threshold, then it will be directly activated to develop the required response. On the other hand, if a B cell matches the antigen with low affinity below the threshold, then it needs the help of a T cell (T helper) in order to get activated, and here we talk about a process called indirect activation. In case of T cells, activation will take place if there is a correspondence between a T cell and MHC molecule that contains a fragment of the antigen.

3. Research Background

AISs are adaptive and evolutionary systems inspired by multiple immune theories applied to solve complex real world problems in various domains. MANET security is one of the most important application domains of AISs, so immune concepts, principals and models are used to provide an alternative approach to enhance MANET security.

AIS started in the mid 80s by Farmer, Packard and Perelson (1986) and then later AIS became an independent domain and gained more importance in the 1990s. Actually, researchers were motivated by some attractive immune foundations such as pattern recognition, memory, learning capabilities and the highly distributed and adaptive structure of immune mechanisms. AISs require bringing together both engineering and computer sciences with transformed complex immunology disciplines and processing them in an interdisciplinary manner. Several interdisciplinary researchers have conducted collaborative efforts on extracting useful immune mechanisms which has lead to a good amount of immune inspired algorithms. For instance, four major artificial immune algorithms are to be distinguished: 1) Negative Selection Algorithm (NSA), 2) Clonal Selection Algorithm, 3) Artificial Immune Network, and recently 4) The Danger Theory and Dendritic Cell Algorithm. An overview of the basic mechanism of some artificial immune theories is given in the following sections.

3.1. Negative Selection Algorithm

Forrest *et al.* [4] proposed in 1994 the Negative Selection Algorithm based on the discrimination between self and non self. The abstraction here is done from the T cells generation process where only T cells that do not match to any self pattern can survive and get to the maturation stage. The anomaly detection process consists of three main phases: The definition of self dataset, then the generation and filtration of detectors since only those that tolerate self elements are kept, and finally the control and detection of abnormal or non self elements.

3.2. Clonal Selection Algorithm

Castro *et al.* [5] proposed in 2000 the Clonal Selection Algorithm CSA. The algorithm then becomes known as CLONALG which is inspired by the clonal selection theory and affinity maturation principles including selection, cloning, memorization, mutation and reselection. The abstraction can be found in the process when a lymphocyte is selected and gets to bind to a foreign antigen. The cell then undergoes a proliferation process and results in a huge number of clones. These clones get affinity maturation where they can differentiate into plasma and memory cells. Plasma cells

produce antibody molecules, while memory cells benefit from an extended lifetime in order to anticipate any future recognition of the same antigen.

3.3 Danger Theory & Dendritic Cell Algorithm

Danger theory is a recent immunological discovery proposed in 1994 by Matzinger [6]. It states that the response of the immune system to pathogens is triggered following presence of danger signals rather than the discrimination between self and non self elements. Danger signals are emitted from the body tissue when it undergoes a pathogenic death [7].

Aickelin *et al.* [8] proposed the implementation of this theory as an AIS model to improve the performance of previously existing models. This has lead to the emergence of a second generation of AISs named "the danger project" [8] [9]. The Dendritic Cell Algorithm (DCA) is one of the most important contributions in this sense [10] [11]. DCA is based on a metaphor that utilizes the role of dendritic cells (DCs).DCs are immune cells defined as antigen presenting lymphocytes that play a key role in controlling the immune system's response. They are responsible for the initial detection of intruders and are responsible to process existing alarm signals.

The AIS researchers' community has produced several variations of immune inspired algorithms and computational tools in order to solve real world problems and mainly computer security problems; for example, Pattern Recognition Receptor Model, humoral immune response [12], dendritic cell functions and Danger Theory [9]. However these researches are still immature, under development, and not yet effectively exploited in the industry. Jim & al have reviewed most of the immune inspired algorithms and their use in mobile ad hoc networks [13]. Ishida [14] as well reviewed diverse immune network models and discussed the benefits of each approach.

4. Security Attacks on AODV

Ad hoc On-Demand Distance Vector (AODV) routing protocol is a reactive routing protocol that creates and maintains routes between source and destination nodes only when needed. When a node needs to communicate, it sends route discovery messages called Route Request (RREQ) in order to establish the shortest path with the desired destination. AODV has gained a large popularity as an important routing protocol for MANETs. It is known to perform well at all movement speeds and all mobility rates. It is a reactive protocol with low complexity and reduced amount of routing information and small packets sizes. There are four types of routing messages: RREQ: Route Request, RREP: Route Reply, RERR: Route Error, RREP-ACK: Route Reply Acknowledgement. In fact, AODV is based on the use of source/destination sequence number (SN) to determine the freshness of a route and to be used also for loop prevention. Route discovery and route maintenance are then the major operations of AODV.

Security in MANET is a highly challenging issue since there is no central line of defense. Moreover, wireless communication adds more challenges to security issue, and brings more diversified attacks compared to wired networks. As a result, developing efficient security solutions always should start by analyzing and understanding different kinds of possible attacks [15]. Actually, these attacks can be classified into internal and external attacks; external attacks are performed by nodes not belonging to the network in order to make network services unavailable or to send false routing information, while internal attacks are originated from compromised nodes that belong initially to the network but then have undergone unauthorized access and still impersonate as authentic node. In fact, internal attacks are usually hard to detect compared with external attacks.

Routing in MANET is done in a cooperative manner where nodes collaborate with each other to ensure the transmission of emitted traffic between source nodes and desired destinations. It is then clear that if one of the cooperative nodes becomes malicious, the whole network turn to be at risk. Also, AODV like other routing protocols can be subject to network layer attacks that intent to prevent the normal use of routing protocols, and then attackers can stand in the middle of a communication and absorb or reroute exchanged data as illustrated in Figure 3.

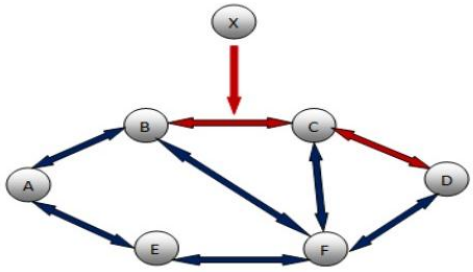


Figure 3. Routing Attack by Malicious Node

In addition, attackers can create loops and overflow routing tables in order to cause network congestion. Indeed, resource consumption or flooding attacks, and packet dropping attacks are some of the most important attacks that AODV is exposed to.

Resource Consumption Attack: Resource consumption attack, also known as the sleep deprivation attack, happens when a compromised node can intentionally attempt to consume battery life of the victim node by requesting excessive route discovery, or by forwarding unnecessary packets.

Packet Dropping Attack: In AODV, the route discovery process between a source S and a destination D take steps described in Figure 4. If a node wishes to start communicating with a destination node, first it checks its routing table to verify if there is a current route to the destination. If positive, the node forwards the packet to the next hop following the path given by the routing table. On the other hand, if no fresh route exists, the AODV starts the routing discovery by having the source node broadcast a Route Request message (RREQ). Whenever an intermediate node has a fresh route to the destination, it generates a Route Reply message (RREP) and sends it back to the source node. Otherwise, The RREQ is rebroadcasted by intermediate node until it reaches the destination node. The route discovery process can be considered as completed only when a RREP that contains the path from source to destination arrives at the source node.

Figure 4. AODV Routing Protocol Processes

Before a node can start a packet dropping attack, it must first get involved in the routing path. To do so, malicious node breaks the route discovery rules given by the routing protocol and lies to S by advertising itself as having the shortest path to D and sends back a RREP to D. S then starts sending data packets to D through the malicious node. In fact, a node can get inside the route using multiple kinds of attacks such as Black hole attack, Gray-hole attack, Rushing attack, Sink Hole attack, and Link Withholding attack.

The design of AODV as well as other routing protocols in MANET assumes that all network members should participate to forward all packets as described by the given routing protocol. This is an unrealistic expectation especially in an open environment like MANET since there is a vulnerability of having network nodes not forwarding packets adequately or even definitely dropping them to prevent establishment of good network communications. The next section proposes an artificial immune system based on the combination of multiple immune theories to address Packet dropping attacks in AODV; the proposed algorithm is then integrated to the AODV routing protocol. So, network simulation 2 (NS2) is used to evaluate the performance of the network in presence of Packet dropping attacks. Moreover, network performance is measured through some parameter such as Detection Rates, False Positive Rates, Packet delivery Ratio, Throughput, End to End Delay, and Control Overhead. Obtained results are compared to the Secure AODV.

5. Combined Immune Theories Algorithm

5.1. Involved Immune Theories

This paper proposes the use of an algorithm named “Combined Immune Theories Algorithm” (CITA) to protect MANET from Packet dropping attacks [16] [17]. CITA combines three basic immune theories and some immunological concepts to provide a better security model that can address security attacks and MANET threats. As a matter of fact, the involved immune theories are: 1.Negative Selection, 2.Clonal Selection, 3. And Danger Theory. Thus, network performance and security parameters are then measured in presence of Packet dropping attack.

Negative Selection Algorithm (NSA): as proposed by Forrest *et al.* [4] is based on the discrimination between self and non-self. In the case of the proposed algorithm CITA, Negative selection is used in the network bootstrapping stage when a set of network nodes (self nodes) intend to establish network connections between themselves. During this learning phase, each node generates randomly a set of

detectors (adjacent detectors) to be used by CITA in order to best protect the network. Generated detectors are firstly Immature Detectors (IMD) that undergo maturation phase through Negative Selection in order to eliminate detectors that can match with previously defined self nodes. Only mature detectors that tolerate to self data items are kept.

The use of NSA is very useful in term of filtering the detectors population; it allows the detection of unknown intruders even without any prior knowledge of their structure. Again, this is why NSA has gained a very large popularity among AISs, but it has shown some weakness especially in term of scalability and coverage. As a solution, CITA Algorithm proposes the integration of other immune theories and concepts such as the Clonal selection and Danger theory in order to address NSA weak points.

Clonal Selection: as proposed by Decastro [5], the algorithm is based on the metaphor abstraction of the proliferation of valuable immune cells that are responsible of any intrusion detection. Also, the immune memory concept is used in this sense since a set of these valuable immune cells, called immune memory cells, with extended lifetime is produced and kept as gene library. likewise, adaptive immunity, also known as secondary response of the Human body, then uses these specific immune memory cells to trigger a quick response whenever the same and already known virus reenter the body. Similarly in our algorithm, if a real detection takes place, the corresponding detector gets cloned and a set of Memory Detectors (MMD) is added to the detectors population. The use of memory detectors in CITA as the first band will help to reduce the complexity of the algorithm, and will allow a quick exclusion of intruders.

Danger Theory as proposed by Matzinger [9-11], the theory states that immune response is not only triggered due to the presence of non self patterns, but it is triggered as well by the presence of damage that can occur in plasma cells. At this point, biologists proved that no immune response is initiated even in presence of some foreign patterns inside the human body such as food proteins and useful bacteria, and that the response is due to presence of some chemical secretions of dead cells, known as alarm signals, that are used to sense the presence of danger. Hence, two types of alarm signals are to be distinguished, Apoptosis is an alarm signal received by dendritic cells if cells undergo normal programmed death, and necrosis is a signal received when cells undergo a pathological death. The proposed algorithm also uses alarm signals (Safe signal, Danger signal, PAMP, and inflammatory signal) as part of the monitoring process of normal or bad behavior of network nodes. A lightweight version of Dendritic Cell Algorithm (DCA) is only used to correlate these input signals in order to evaluate the context information. Accordingly, this context information can be either “safe” or “Dangerous”; CITA then will act differently based on the sensed context as will be explained later. If the context is dangerous, CITA looks for real detections (True Positives: TP) and starts the detection process to isolate malicious nodes, but if it is safe, then CITA looks for false detections (False Positives: FP) to suppress the corresponding detectors.

All in all, CITA is an algorithm that intent to combine all these three immune theories and concepts in order to best simulate the immune defense and to enhance MANET security. Figure 5 gives an overview of how CITA can be run on a single node involving all these immune theories and concepts.

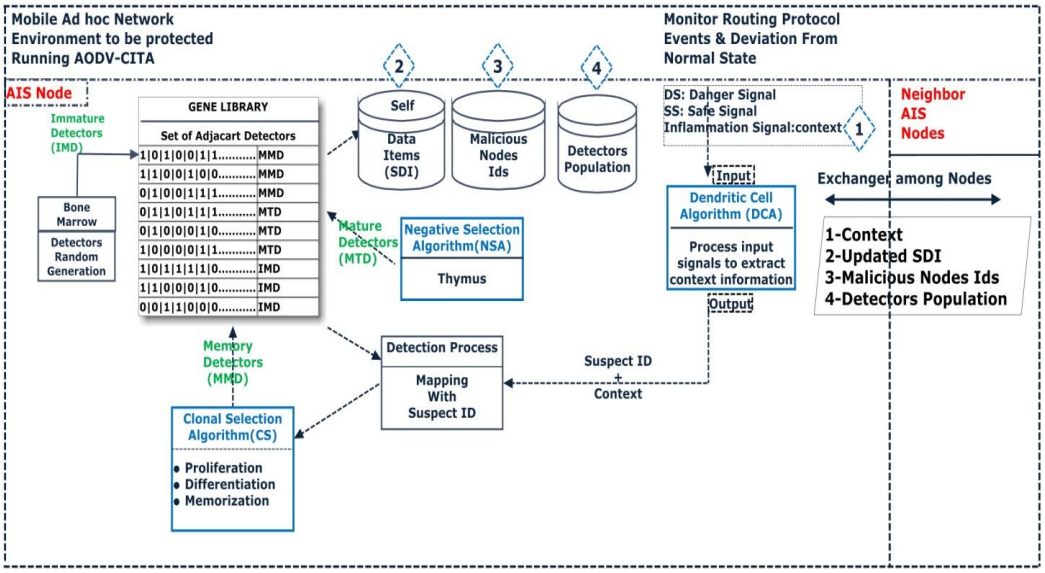


Figure 5. An Overview of CITA Running on a Single Node Involving Different Immune Theories and Concepts

5.3. CITA Algorithm

Combined Immune theories algorithm (CITA), is an active intrusion detection system based first on monitoring and detecting deviations from normal behaviors to extract context information before it can use it to initiate an appropriate detection process. Then, two specific and different detection processes are used according to the presented context involving the detectors population. If the context is safe then CITA looks for False Positive (FP) detections, but if it is dangerous, then CITA looks for True Positive (TP) detections. The last step then will be to exchange results and updated data with all neighbor nodes. Each node stores and exchanges four updated small data amounts related to:

- Sensed Context information.
- Self Data Items (SDI): that represents the list of self nodes identifications, or network nodes Ids.
- Malicious Nodes Ids: that represents the list of nodes Ids that have been detected as malicious nodes.
- Detectors Population: In addition to local adjacent detectors, each node keeps and updates the whole detectors population to use it in the detection process if needed.

The proposed CITA algorithm performs its role through four major stages as explained below:

1. **Learning stage** is the first step when network nodes undergo the bootstrapping stage with a limited number of predefined network nodes. Each node starts by generating an initial set of immature detectors that will undergo the maturation stage through NSA while checking every single detector with all self data items in order to keep only detectors that tolerate self items as shown in Figure 6. The set of updated detectors is exchanged with all neighbors.

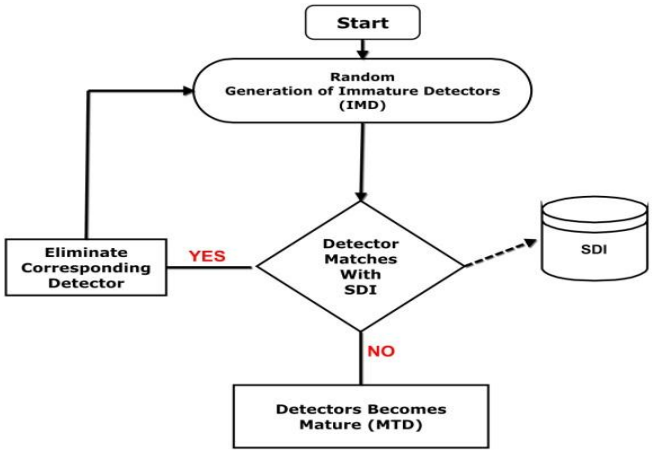


Figure 6. Maturation Stage through NSA

2. **Extraction of context information** is another important step where CITA plays its role as a monitoring system to detect deviations from normal behaviors by comparing real parameters values with allowed intervals of reference for those parameters. Then, a set of alarm signals are defined such as Danger signal (DS), Safe Signal (SS), inflammatory input signal, and PAMP signal; the definition of these alarm signals depend on the considered attack. In this paper they will be defined later to deal with Packet Dropping Attack. A lightweight version of DCA uses these alarm signals as input signal, DCA then correlate these signals among each other just to decide about the context information if is safe or dangerous.

3. **The detection process** is based on the mapping between detectors represented by binary strings of 24 bits and the given node ID which is represented by a binary string of 8 bits. The matching rule used is r-contiguous bits with r=8. A detector can match up to 17 nodes by transiting the starting position of the matching rule. Two different scenarios are adopted depending on the context information; if the context is safe then CITA looks for False Positive (FP) detections in order to eliminate the corresponding detectors and avoid any False Positives in the future, but if it is dangerous, then CITA looks for True Positive (TP) detections in order to exclude the intruder.

4. **Exchange Data with neighbors,** after CITA is run on a node many changes can occur on the local stored data:

- CITA may recognize some network nodes as malicious nodes and update the list of malicious nodes Ids.
- A new harmless inserted node can be added to the list of self nodes;
- Context can change from safe to dangerous;
- The local adjacent detectors get more filtered and get added to the updated list of detectors population.

All these changes that happen on a node after running CITA are sent to neighboring nodes so they can also update their own stored data in a cooperative and auto distributed manner. This process allows network nodes to share the results of their experience with other network nodes to save considerable effort, time and battery resources.

5.4. Monitoring & Reputation Systems

The simulation of the proposed algorithm is quite a complicated task, since it raises the need to use a monitoring system to sense nodes deviations from normal behaviors. As a matter of fact, each network node monitors the next node after forwarding any data packet since the next node is under its transmission range and it is able to hear and capture forwarded packets. The monitoring then consists of a node registering any packet before it sends it to next hop and setting the timeout for the packet. The node then verifies if the next node forwards the packet within timeout without modifying or dropping the packet. If the packet is considered as dropped by next the node, then the monitoring system reports this information to the reputation system to change the scores of the related node.

The reputation system is the system responsible of cumulating positive and negative scores related respectively to good and bad behaviors. Whenever the cumulated score within a period is outside the accepted boundaries then a dangerous alarm signal related to the suspicious node is generated to trigger the proposed CITA algorithm to be run on a single node. CITA is triggered also when context information exchanged between neighbors is dangerous.

5.5. Integration of CITA with AODV Routing Protocol

CITA is an algorithm that gets triggered on a network node whenever the reputation system generates an alarm signal related to nodes deviations from normal behaviors (Danger signal). Also, it can be triggered following the reception of dangerous context information sent from neighbors (Inflammation Input signal). Actually, CITA can be used with various routing protocols that apply to MANET; however, CITA is much more compatible with reactive routing protocols since RREQ is sent only when a node intents to establish a communication with a destination node. Consequently, it gives better results especially in terms of energy consumption.

Ad-Hoc On-Demand Distance Vector (AODV) is a reactive routing protocol where routes information is only transmitted by nodes on-demand [18]. 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 reply later by sending back an up to date or fresh route between source and destination called Route Reply (RREP). As soon as AODV receives all active routes, it chooses the shortest path. The source node sets a timer to wait for a RREP before it can broadcast again a RREQ packet through the network.

In the following sections, we address the use of CITA Algorithm to enhance AODV in term of security and especially to avoid Packet Dropping Attacks already explained in previous sections. The Monitoring process is triggered on a node whenever a packet is sent from this node in order to track next hop behavior before it can report this information to the reputation system. The rest of other processes like the extraction of context information and the detection processes then are initiated following either a danger signal generated by the reputation system or by the reception of dangerous context information from neighboring nodes. If suspicious node then is recognized to be a malicious node, then it will be added to the list of malicious items and the results will be exchanged with all neighbors. The malicious node then will be excluded from fresh routes and won't participate in any network communications.

.

6. Results and Discussions

6.1. Simulation Environment and Parameters

Network Simulator-2 version 2.35 (NS2) is selected to be the simulation environment. It is a free simulation tool that runs on Linux operating systems; it has gained a large popularity among other network simulations. NS2 supports the implementation of MANET with all related routing protocols and most of existing attacks already embedded. It is an extendable tool since it allows users to access C++ packages in order to create new class libraries with all needed methods and properties, as they can modify existing code. OTCL script is also available to configure all network simulated parameters and events, such as the number of nodes, simulation time, simulated area, type of mobility, nodes movement scenario, routing protocol, transmission rate, and nodes misbehaviors...etc.

The adopted simulation scenario uses 50 mobile nodes, where initially only 20 of them are involved to establish a trusted network that undergoes the bootstrapping stage. In fact, this starting phase of 100 seconds is a learning stage where nodes start generating local adjacent detectors and exchange them with neighbors to build the detectors population that get filtered through NSA and only detectors that tolerate self nodes are kept. Then, an initial topology is created, and each node updates self data items represented by those initial nodes IDs. The rest of the scenario takes 800 seconds and describes the insertion of the other 30 nodes progressively while mobile nodes keep moving following the Random Way Point (RWP). After each 45 seconds two nodes get inserted, one of these two nodes is normal with no bad behavior, but the second inserted node is a predefined malicious node that starts dropping packets.

6.2. Setting up some Initial Parameters

The definition of alarm signals, as well as the number of adjacent detectors needs to be set as initial parameters before we can start simulating CITA Algorithm. Also, the number of adjacent detectors to each dendritic cell is chosen to be 10 detectors 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.

The DCA part of CITA Algorithm requires first the definition of what Alarm signals are in order to correlate these signals together and to extract context information. In fact, the definition of these signals is based on the nature of the studied attack. Malicious nodes in this study use Packet dropping Attack since they keep dropping useful packets. Alarm signals then are defined as following [19]:

- PAMP Signal: If high rates of dropped packets are registered on a suspicious node, this indicates strongly the presence of Packet dropping Attack.
- Inflammation input signal: If suspicious node is already recognized to be a malicious node by one of neighboring nodes.
- Danger signal: If context exchanged from a neighboring node is dangerous, then this adds strong confirmation that there is presence of an attack from neighboring node.
- Safe Signal: If data packets delivery and routes discovery processes succeeds, this means fairly absence or failure of a Packet Dropping Attack.

In effect, performance analysis will be based on the results of captured data during the execution of the described scenario. In order to compare obtained results, the same scenario is run in two experiments. The first experiment is done using the secure AODV (SAODV) routing protocol [20], and the second one is conducted using CITA

algorithm implemented with AODV. Results then are compared for different network configurations. For each experiment, simulations are repeated five times and the average is taking into consideration to avoid the use of an overstated positive scenario.

6.3. Performance Parameters & Evaluation

The performance of MANET depends on multiple network parameters such as the ability to detect intrusions, and the amount of data exchanged between nodes to ensure reliability, the available bandwidth, data delivery, packet loss, the delay...*etc*. This paper investigates the evolution of a variety of metrics in presence of packet dropping attacks in order to evaluate network performance. Simulations are conducted using both CITA-AODV and SAODV while assuming that links between nodes are bidirectional. Performance metrics that have been used with corresponding results are shown below:

6.3.1. Detection Rate: This parameter reflects the effectiveness of the proposed intrusion detection system in terms of preventing attacks from malicious nodes; it is also called True Positive detection rate and measures the percentage of what extent real detection can be recognized. In fact, the studied intrusion detection system aims to isolate and exclude all malicious nodes; it considers that every packet originated from any recognized malicious node as an attack and consequently this packet should be dropped. Then, Detections are represented by intentionally dropped packets; a higher value of the detection rates corresponds to a better performance of the intrusion detection system. Detection Rate is defined as the ratio of Total number of attacks being correctly detected to the total number of attacks being occurred.

DR (%) = (Σ No. of detected attacks / Σ No. of occurred attacks)*100

Obtained results are as follows:

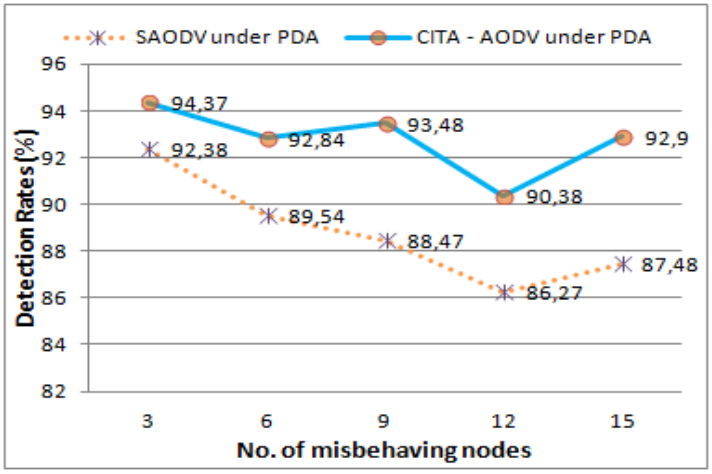


Figure 7. Detection Rates vs. Number of Misbehaving Nodes

Figure 7 illustrates the average detection rates for both SAODV and CITA-AODV according to the number of inserted malicious nodes. The studied scenario implements severe attacks since the number of inserted malicious nodes keep increasing until 15 malicious nodes. After a node is being recognized by CITA-AODV as a malicious node, all packets originated from that node are intentionally dropped and marked as "Attack". The graph shows a remarkable increase of the proposed CITA-AODV in term of detection rates; and CITA-AODV proves a sustainable resistance against serious attacks. Actually, the average detection rate of CITA-AODV is of 92.79% against 88.82% tracked for SAODV. Both CITA-AODV and SAODV get influenced

inversely proportional by the increasing number of packet dropping attacks; except that auto adaptation and auto learning philosophy of CITA-AODV allow it to isolate suspicious nodes very quickly after a certain time thanks to the use of Memory detectors.

6.3.2. False Positive Rates: False Positive Rate (FPR) represents false detections identified by the system when normal nodes with no bad behaviors are tracked as anomalies. FPR is given by the ratio of falsely identified attacks to the total number of normal events. A reduced value of FPR means high precision of implemented IDS.
FPR (%) = (Σ No. erroneous attacks / Σ No. of normal events (all packets originated from normal nodes))*100

Obtained results are as follows:

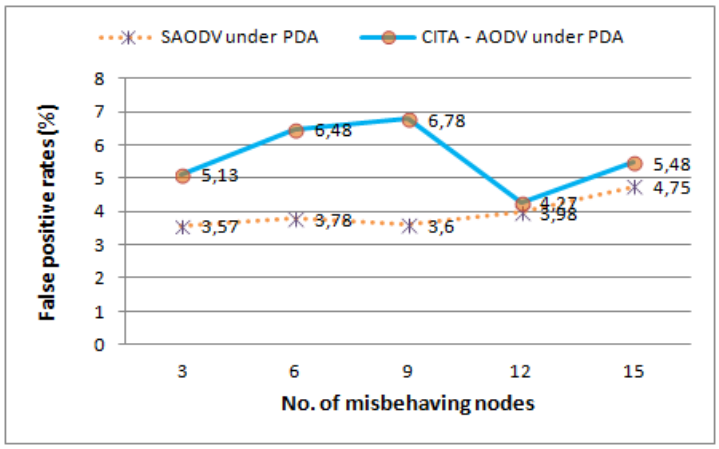


Figure 8. False Positive rates vs. Number of Misbehaving Nodes

Figure 8 illustrates the false detection rates according to the number of inserted misbehaving nodes for both CITA-AODV and SAODV while running the same predefined scenario. Then, high rates of False Positives are registered for CITA-AODV compared to those of SAODV. Obviously, this is not a good performance since the goal is to minimize FPR in order to have a much better precision of the detection process. In fact, the average tracked for CITA-AODV is of 5.62% while SAODV registers an average of 3.93%. These results can be explained by the fact that almost 60% of packets dropped in MANET are either due to congestions, wireless link transmission media or nodes mobility. Then, the monitoring system tracks most of these drops and reports them to the reputation system; dangerous alarm signals are more often sent, a fact that influences the nature of the extracted context. In fact, multiple sensed alarm signals can lead to the increasing rate of false positives. So, a solution to this problem could be to investigate better trusting threshold to avoid excessive false detections and to provide more tolerance.

6.3.4. Packet Delivery Ratio (PDR): Packet delivery ratio illustrates quantitatively the level of successfully delivered packets to the desired destination. It is given by the ratio of total number of delivered packets to the total number of sent packets. The greater value of PDR corresponds to a better performance of the protocol.

$$PDR\ (\%) = (\sum \text{No. of packets delivered} / \sum \text{Number of packets sent}) * 100$$

Obtained results are as follows:

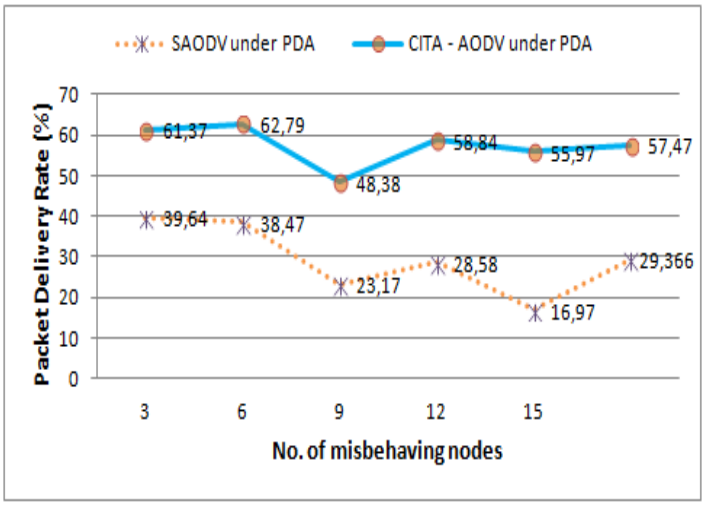


Figure 9. Packet Delivery rates vs. Number of Misbehaving Nodes

Simulation results of Packet Delivery Rates are given by Figure 9. The studied Packet Dropping Attack has a direct impact on the ratio of the total number of successfully delivered packets to the total number of sent packets. Actually, the main goal of this attack is to keep dropping packets, and the chosen scenario is very severe as well. It is crystal clear that the proposed CITA-AODV maintains a good performance regarding this network performance metric compared to SAODV. An average of 57.47% registered for CITA-AODV against 29.36% for that of SAODV.

6.3.5. Throughput: Throughput represents the transmission capacity of a network by measuring successful delivered packets in a given time interval; it is related to available transmission rate and available bandwidth, as it is influenced by congestions, flooding, and routing control overhead. Also, Throughput is given by the fraction of successfully received bits for all network nodes during a period of time. Certainly, high throughput corresponds to better performance

$$\text{Throughput} = \Sigma \text{ No. of received bits} / \Delta t \text{ (Stop Time - Start Time)}$$

Obtained results are as follows:

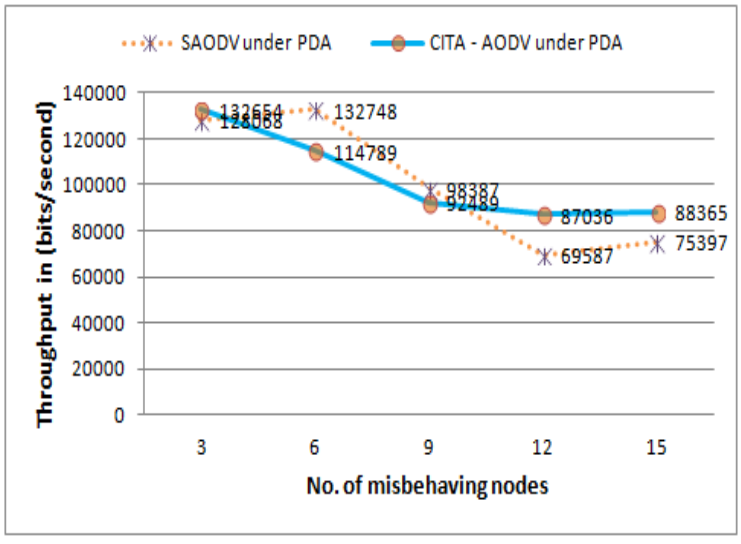


Figure 10. Throughput vs. Number of Misbehaving Nodes

The throughput metric measured for both CITA-AODV and SAODV is shown in Figure 10. It is easily remarkable from the graph that the throughput is impacted by the increasing number of attacks for both protocols. In fact, Packet size and the number of packet sent by a single node are also two other factors that affect the throughput of the network. Our predefined scenario considers two packets of 128 bytes each sent per second by every single node. Obtained results show that there is no big difference in term of throughput between CITA-AODV that registers an average of 103066.6 bits/s and that of SAODV that registers an average of 100837.4 bits/s, except that CITA-AODV succeeds in keeping a stable throughput by the end of the simulation even with an increasing maintaining number of attacks. This stability can be explained by the auto-adaptive character of the implemented intrusion detection system.

6.3.6. Control Overhead: Control Overhead illustrates quantitatively how much routing packets are required by a protocol. It is clear that every intrusion detection system adds more control packets that are responsible for misbehavior detection in the network. Again, Control overhead is calculated as the ratio of the number of routing packets to the number of delivered data packets. Low control overhead reduces the complexity of the network and then corresponds to a better performance.

$$\text{Overhead (\%)} = (\Sigma \text{ No. of control packets} / \Sigma \text{ No. of delivered data packets}) * 100$$

Obtained results are as follows:

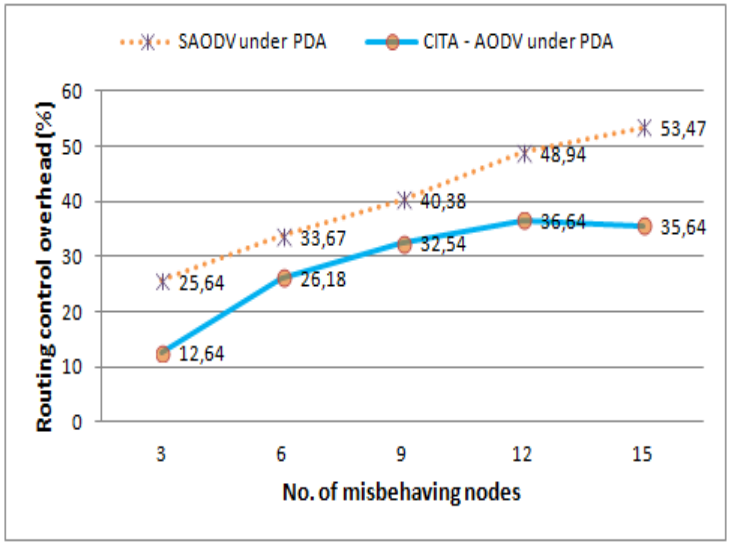


Figure 11. Routing Control Overhead vs. Number of Misbehaving Nodes

Figure 11 shows that routing control overhead increases proportionally to incremented number of malicious nodes inserted for both CITA-AODV and SAODV. The reason behind this conclusion is that for both tested protocols, malicious nodes once detected are isolated and excluded from rerouting process. So, source nodes don't establish routes through malicious nodes. Actually, all routes already established that contain a malicious node are considered as failure links which results in more route discoveries; this increases routing control overhead. However, there is an increase in control overhead for SAODV compared to that of CITA-AODV since SAODV registers an average of 40.42% while CITA-AODV registers an average of only 28.72%. The increasing amount of control overhead for SAODV is due to the use of asymmetric key cryptography that requires extra bytes to store hashes and digital

signatures. Ultimately, control overhead is also influenced by increased mobility and higher speed of nodes which can lead to more link failures.

6.3.7. End to End Delay: End-to-end Delay represents the average time taken by data packets to transit from source nodes to destinations for all active connections. All probable delay included is either caused by buffering during routing discovery process latency, or by data packet transmission queue. Actually, only data packets that are successfully delivered to destinations are counted, and better performance of the protocol is obtained when lower value of End to End Delay is measured.

$$\text{End to End Delay} = \sum (\text{arrive time} - \text{send time}) / \sum \text{No. of active connections}$$

Obtained results are as follows:

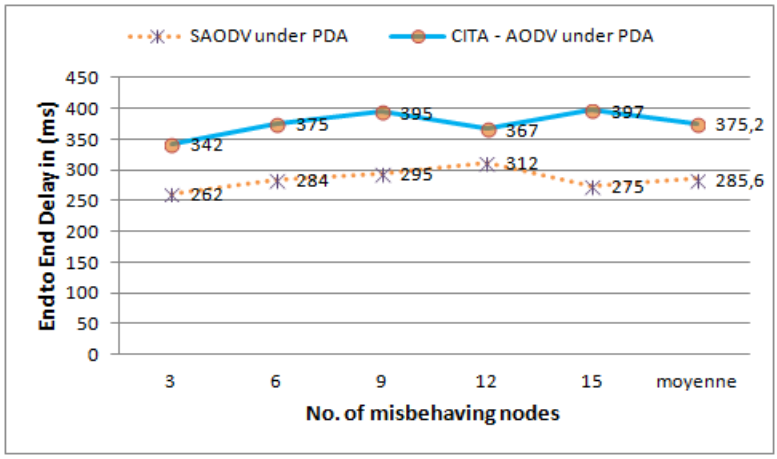


Figure 12. End to End Delay vs. Number of Misbehaving Nodes

End to End Delay as given by Figure 12 shows a small increase in the time required for a first data packet to transit to the desired destination after the source node broadcasts RREQ message. Obviously, in presence of malicious nodes, Packet delivery requires more processing time to compute and verify which nodes are responsible for the attack in order to block them and establish new links between senders and receivers. CITA-AODV registers an average of 375.2 (ms) against 285.6 (ms) registered by SAODV. The monitoring and reputation systems altogether provide useful signals in order to process them and to extract context information; the detection process of CITA checks if the received packets are originated from an already listed malicious node, if so, it processes the matching between detectors population and suspicious packets received; all these steps together require a little more processing time.

7. Conclusions and Perspectives

The proposed Algorithm is an intrusion detection system (IDS) based on the use of a population of detectors distributed and exchanged among network nodes. The proposed IDS is named Combined Immune Theories Algorithm (CITA) since it abstracts metaphors from three major immune algorithms that are NSA, CSA, and DCA. The algorithm consists on a set of operations against detectors population according to the context information revealed by DCA. Those operations can be detectors maturation, matching, cloning, suppression, substitution, memorization, and so on. These operations then approve the filtration of this detectors population in order to be very

precise which allows the proposed CITA to be an auto adaptive system, auto learning and an evolutionary algorithm. All in all, simulation results show better performance of the proposed CITA algorithm embedded with AODV routing protocol in presence of Packet Dropping Attacks compared to Secure AODV as given in Section 6.3. Network performance is measured based on DR, FPR, Throughput, PDR, End to End Delay, and Control Overhead. For the most part, the objective of the proposed approach is the enhancements of MANET security compared to 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.

Future work will study the performance of CITA in presence of other types of attacks, as it will evaluate other network performance parameters such as Packet Loss, and Mean hop count. Generally, future research will also focus on the definition of a standard normal behavior without considering the nature of attack, in order to make easy the tracking of deviations and malicious acts.

References

[1] Chaki N. and Chaki R., "Intrusion Detection in Wireless Ad-hoc Networks", CRC Press 1st edition, **(2014)**.
[2] Abdelhaq M., Hassan R. and Alsaqour R., "Using dendritic cell algorithm to detect the resource consumption attack over MANET", Software Engineering and Computer Systems, Springer, Berlin Heidelberg, **(2011)**, pp. 429–442.
[3] J. Timmis, "Artificial Immune Systems: A novel data analysis technique inspired by the immune network theory", PhD Thesis, University of Wales, **(2001)**.
[4] S. Forrest, A. S. Perelson, L. Allen and R. Cherukuri, "Self-Nonself Discrimination in a Computer", IEEE Symposium on Research in Security and Privacy, Oakland, **(1994)**, May16-18, pp. 202-212.
[5] L. N. De Castro and F. J. von Zuben, "The Clonal Selection Algorithm with Engineering Applications", Genetic and Evolutionary Computation Conference, Workshop Proceedings of GECCO'00, Las Vegas, **(2000)**, July 8-12, pp. 36-37.
[6] P. Matzinger, "An innate sense of danger", Seminars in Immunology, vol. 10, **(1998)**, pp. 399-415.
[7] Matzinger P., "Friendly and dangerous signals: is the tissue in control?", Nature immunology, PMID: 17179963, vol. 8, no. 1, **(2007)**, pp. 11–13.
[8] Aickelin U., Bentley P., Cayzer S., Kim J. and Mcleod J., "Danger theory: The link between AIS and IDS?", Artificial Immune Systems, Springer, Berlin Heidelberg, **(2003)**, pp. 147–155.
[9] Aickelin U. and Cayzer S. "The Danger Theory and Its Application to Artificial Immune Systems", no. arXiv. 0801.3549, **(2008)**.
[10] J. Greensmith, "The Dendritic Cell Algorithm", Thesis Submitted for the Degree of Doctor of Philosophy, University of Nottingham, **(2007)**.
[11] Greensmith J., Aickelin U. and Cayzer S., "Introducing dendritic cells as a novel immune-inspired algorithm for anomaly detection", Artificial Immune Systems, Springer, Berlin Heidelber, **(2005)**, pp 153–167.
[12] D. Dasgupta, S. Yu and N. S. Majumdar, "MILA – multilevel immune learning algorithm", in: Genetic and Evolutionary Computation Conference (GECCO 2003), Chicago, IL, USA, **(2003)**.
[13] L. E. Jim and M. A. Gregory, "A Review of Artificial Immune System Based Security Frameworks for MANET", Int. J. Communications, Network and System Sciences, vol. 9, **(2016)**, pp. 1-18.
[14] Y. Ishida, "Immunity-Based Systems: A Design Perspective", Springer Science & Business Media, **(2004)**.
[15] A. Gagandeep and P. Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), **(2012)**.
[16] A. Khannous and F. Elouaai, "A new approach to artificial immune system for intrusion detection of the mobile ad hoc networks", IJCA journal, vol. 92, no.15, **(2014)**.
[17] A. Khannous and al, "Securing MANETs using the Integration of concepts from diverse Immune Theories", JATIT, vol. 88, **(2016)**.
[18] A. Gupta, H. Sadawarti and A. Verma, "Performance analysis of AODV, DSR & TORA routing protocols", IACSIT international journal of Engineering and Technology **(2010)**, pp. 226-231.
[19] M. Abdelhaq, R. Hassan, M. Ismail, R. Alsaqour and D. Israf, "Detecting Sleep Deprivation Attack over MANET Using a Danger Theory-Based Algorithm", IJNCAA, vol. 1, **(2011)**, pp 534-541.
[20] D. Cerri and A. Ghioni, "Securing AODV: The A-SAODV Secure Routing Prototype", In Communications Magazine, IEEE, vol. 46, no. 2, **(2008)**, pp. 120-125.

