ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CO-Operative Immune Model for the Mobile ADHOC Networks Based on the Immunizing Technique

Mrs. A. Naveena
Assistant Professor,
G. Narayanamma Institute of Technology & Science,
Hyderabad.

Dr. K. Rama Linga Reddy
Professor and HOD,
G. Narayanamma Institute of Technology & Science,
Hyderabad.

Abstract:

It is the perfect place to secure the mobile ad-hoc network design parameters, the proposed framework is interesting products. Another future research dealing with the unknown attacks by increasing the accuracy and speed of the pro-immunization is to improve immunization protocols. Coordinate attacks on other tests, evaluations selfs problems, complexity, optimization, and the use of the actual Time is also left for future work . The experimental results of detecting and protected as WiMAX networks, mobile ad networks from disrupting the proposed reduction of the Co- operative immune to the attacks confirm the effectiveness of the model .

MAMET Secure communication is also a demand for different types of vulnerabilities, suffers from the problem. Less network infrastructure , special features , such as the absence of official orders , the movement of nodes in a variety of dynamic random attacks. The attacks became more intense . A lot of hassle- free communication protocols and algorithms developed in order to secure , but is still in demand due to the growing use of MANET is the lack of protocols have been fully secured . In this paper we present an algorithm for coordinated attacks on the modified AODV .

Index Terms:

cooperative immune model, collaborative black hole attacks, Tri-tier cooperative immune model., dynamic source routing (DSR), gray hole attacks, hostile node, mobile ad hoc network (MANET).

I.INTRODUCTION:

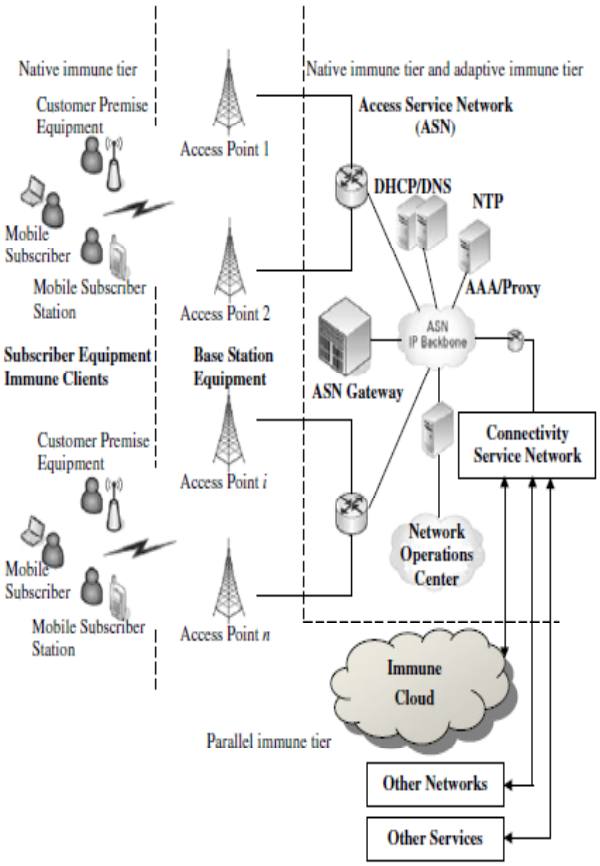
We are here to discuss security issues, with a focus on collaborative attacks, Access (WiMAX) Worldwide Interoperability Microwave scene[1].

Non-DOCSIS, DES Have, and AES WiMAX protocol suite has a large number of protocols, but not limited to. We present a brief WiMAX standard and its vulnerabilities. We Protocol Suite, WiMAX and WiMAX systems and protocols that person to discuss cooperative attacks[2]. WiMAX attack scenarios we present, in general , there are several , including : an increase in their computation power to break and bring a large number of attack WiMAX protocols ; Sybil attacks against routing attacks , and a dual - core machines , decision-making , assembling a sufficient number of attack is affected ; And a wide range of issues[3,4], including interoperability between different protocols typical WiMAX / WiFi, Description and exploitation of WiMAX / LAN deployment practices scenarios. ad networks rely on the cooperation of nodes to establish communication with the ins malicious nodes within the entire network can be compromised.

If they collaborate the devastation is even worse. They combined efforts of attacks against the target of the attack was the victim of a cooperative attacks are, more than anything else, the devastating effects of single and uncoordinated groups may be more than one wireless environments. In this paper, we discuss the works to be among the attackers , detect and defend against attacks, the attacks show how such environments can be used to discuss the implementation of the cooperation and the most important forms of machine learning techniques and methods of signal processing problems. Visual modeling approach and its calculation method proposed to represent and simulate a kind of adaptive immune system. Adaptive immune system, immune cells and immune molecules etc, because there are models rather than the traditional hierarchical model of the immune system more reliable and suitable for visual simulation, is proposed. Systemic immune system, mainly the characteristic of the adaptive immune tire is the tire and the level of immune cells[5].

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Tri of the immune system - the tire model with the construction of an artificial immune system is seamless and coherent. At last, simulation, visual modeling approach to the visual result shows that provide an effective way to understand the adaptive immune system. Ad- hoc network nodes are self-managed and can easily join or leave the network at any time to have such a dynamic topology of the nodes are autonomous.



I.COLLABARATIVE ATTACK:

A system of coordinated attacks by attacking at the same time delivering the synchronized attacks . Target of attack by more than one process is running or when the network synchronize their actions violated the cooperative attacks (CA) are formed. It is an attack on every person who may have a special skill , a new generation is under attack . A system, but not necessarily, with the collaboration of multiple attacks occur when more than one disturbed by the attack, which is different from the multiple attacks. Preventive and mechanisms to secure the attacks are only available for personal attacks. Various diseases in the human body, viruses, bacteria, the body's immune system becomes more and more down through a variety of cough, fuel, such as malaria, at a time when attacked.

II.RELATED WORK:

Cooperation defend against attacks, collaborative processes have been recently proposed. For example, Cheung et al. Multiple sub attacks some of the spoils of cyber attacks and the invasion of steps [8] on the basis of warnings about the simple discrete model of the multistep developed a method of attack scenarios. Li et al. Coordinate internal and external attacks [9] constructed a random sample. Yang et al. Cooperation attacks [9] to identify a signature-based model. Multicast, comments topology information and blind detection methods, Hussain et al. Distributed denial-of-service attacks to find a cooperative system [10]. Ourston et al. Hidden Markov models are used to coordinate attacks [11] to detect. Cuppens et al. Some collaborative IDSs every intrusion detection system (IDS) false positives [12] to reduce the number of referrals to the central module has triggered it.

The module comes with all IDSs correlated with the warnings and the entire system to produce more elaborated and general alarm. Linetal. They have a demanding job , [13] which is a comparison of the model to save time and energy , so that the shared information from other nodes in the node that detected the intrusion . Sung Yu et al. IDS is a collaborative work cooperatively proposed for the different types of IDSs[14]. IDS unknown attacks to overcome the disadvantages , especially in the mobile ad-hoc network of immune computational methods , some of which have been investigated for security applications .

Mohamed et al. Mobile ad hoc networks [15], a number of processes for securing the human immune system, providing inspiration for the security architecture presented immune- . Atakan et al. Self- nonselfs recognition and clonal selection is based on the principles [16] in the spirit of the evolution of the immune system, the introduction of opportunistic spectrum access protocol.

One of the foundations of security, threat modeling or destruction of any condition of service, disclosure, modification of data in the form of a system that has the potential to cause harm to the event, and / or refusal to disclose defined as a systematic exploration of the technique, and the results of a vulnerability assessment.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Therefore, the threat modeling or other exploratory techniques to explore the known and potential security vulnerabilities and their effects shall be applied. BAU et al. Security analysis model is illustrated using observation , but analysts manual and the threat model to provide assurance about the absence of attacks in automated theorem - proving system security , including tools , techniques and tools used to evaluate different , Equal to the threat model , the risk of immune theory Matzinger [17] proposed by the theory of this accident , the damaged cells to produce an immune response that separates the signals of danger . In AIS , threats and foreign nonselfs selfs are damaged , so that the nature of the threats are nonselfs . AIS security vulnerabilities, depending on its design .

III.SIMULATION OF COLLABORATIVE ATTACK IN NS2 :

The parameters of the network environment , tools , and some of the values and assumptions follows.- TCP / IP network transmission , IEEE 802.11 b (Media Access Control) MAC, were randomly assigned to 21 nodes , constant bit rate (CBR) of the application , can be described as node mobility network routing protocol AODV run , to use all MANET nodes . This on-demand distance vector NS2 Ad- (AODV) AODV simulation node using the black hole and the hole GRAY is a way to transmit data to a node in a reactive routing protocol, which only you have searched for .Using the serial number of each route entry is a link to the destination from the destination requested by the most promising feature of this protocol.

Route Discovery and Route Maintenance: AODV works in two phases. The way for the discovery algorithm (RREQs) Route requests and uses the root (RREPs) are not messages. The way to the root of the algorithm for the management of Errors (RERRs) and uses HELLO messages. When a node to communicate with another node, it will look for a way out of the table. If you find a legal entry, it uses a different path to the destination node to find the broadcast RREQ to its neighbors. Neighbors RREQ broadcast their neighbors again. Each node is created at the source in a reverse way. Destination or an intermediate node to the destination, but the latest way to continue this process. Node , and then builds a RREP packet and sends it to the node from which the RREQ packet is received .

At each intermediate node is the only way to reverse the RREP packet , and the destination path is constructed as a forward or updated . When the originator of RREP way to complete discovery.

PROPOSED METHOD:

A.COOPERATIVE IMMUNIZATION MODEL AGAINST COLLABORATIVE ATTACKS:

WiMAX network vertex or node set V and edge set with EE 6¼f limited immune graph G = (V, E) is a mobile ad hoc network , such as the representation . In mobile ad-hoc network is an element of V is set for a client, server , or refers to the cloud , and any element of the set E is a client / server and it represents the relationship between one another . It is assumed that the edges of the undirected graph is connected. When starting the system, the mobile ad-hoc network without any attacks on its simple design [9] identified by the representation of space-time, which is common. It also has a unique sequence of discrete time t = 0, 1, 2 represented with assumed that. . ., The timing of some parts of the back or in a local virtual space is a big step forward may be changed, Considering such attacks and attacks warehouse. Wormhole attacks in sequential order , a node is damaged, or removed at any point of time , is safe . in warehouse wormhole attacks and cooperative attacks on two types of attacks are detected and eliminated the problem of defending against attacks. For the calculation of the amount of attacks, defending against attacks following this problem is formulated. The second step is to learn and expendable attacks cooperatively unknown attacks based on the multidimensional feature space is used to determine the level of adaptive immunity. Cooperation reduce attacks, collaborative immunization following the announcement of mobile networks, with the inputs of all the objects in the works. First, the local immune tier mobile ad-hoc network detects selfs of the common components are defined here. As shown in Figure 1. In order to enhance the precision of the self-identity of the usual self-model, the space-time characteristics of the mobile ad-hoc network is a simple, Of the self- detecting space-time characteristics of the state , the common parts of the self are stored in the database .The first step is to find out the results of the immunization selfs much faster than the direct approach to detecting attacks to detect more attacks because of the three-dimensional model of the tire and auto- immune model based on self- identification .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

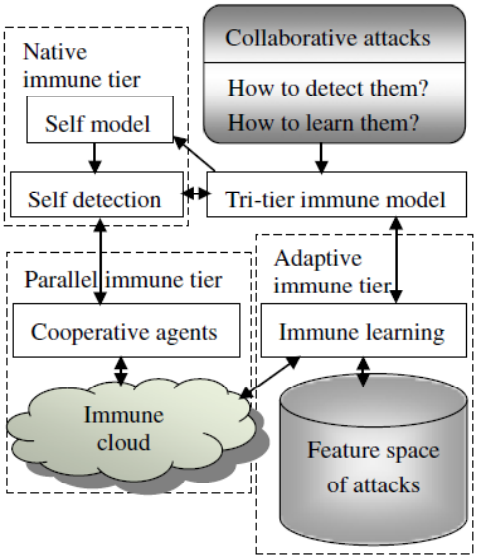


fig 1: Tri-tier cooperative immune model

IV.Secure Tri-tier Immune Model :

Fig wormhole attacks in mobile ad networks, this is not a safe for the proposed three-dimensional model of the immune tire. 1. selfs simple model of local immune tire primarily used to detect attacks by detecting the level of cooperation, that is, cooperative attacks are known or unknown to the network. Important for increasing the efficiency of detecting selfs, and selfs simple model based on the characteristics of the space-time regular nodes.

The second level of the adaptive immune wormhole attacks, network attacks expendable when unknown attacks can be used to multi-dimension feature space. Secure immune immunization process model described below. First, the local immune tier mobile ad-hoc network is a constituent of the normal selfs, detect, and normal states to increase the precision of self-identity for the self-model space-time features.

Compromised nodes of the self - direct the motion of the nodes based detection is more accurate and efficient than the identity of the phrase and the first stage of the model, because the self-self model of self-identity, are important to secure a three-dimensional model of the immune tire. Moreover, when the self-model is damaged, the tire and parallel adaptive immune tier cloud properties of the immune learning nonselfs phrase can be used to detect attacks .

Immune cloud computing infrastructure has been established and is now in the immune computational efficiency and robustness of a new parallel computing system , which is used to increase . In Fig . 1 , the immune learning feature space attacks are made by searching for the most similar attacks . Mobile ad-hoc network of collaborative attacks, the attack is detected at any part of the attack on the immune respect to activate immune responses against the onslaught of information about the node will be sent to the tire .After the attack has been detected in real-time algorithms for searching the database of all known attacks and wormhole attacks expendable in the feature space are identified by comparing their available features. If you have at least a proper record of the search result, then the co-regulation and an easy way to clear the attack, and the attack on the features and collaborative research as a result of the collaboration will be sent to remove the tire is relatively immune to attack, keeping secure mobile ad-hoc network.

Search Result for nothing in return, then an unknown object, such as the invasion of collaborative learning some clever techniques will be learned and grown from the examples of cloud computing and the learning process is built on a partially immune -learning neural network learning based on real-time , etc. should be done. Brain and brain -based learning devices unknown objects with familiar objects to compare and test the unknown to discover knowledge [19]. In recognition of unknown attacks , the immune learning algorithm, the node's attribute information obtained in the first attack , and then it's all in the space of a point feature information is built with the attacks on the feature transforms the data into a feature known attacks by unknown assailants . Then the algorithm similar to the one unknown attack , which is known for the assault class , searches for the best suitable class . The search process is random and is optimal , and the evolution of the immune learning algorithm that can search or non evolutionary built into the solution . After the search returns a optimal solution, the most similar known attack to the unknown one is found. So the type and processing solution for the unknown attack can be calculated with the type of the most similar known attack and both the feature information of the unknown attack and the most similar known attack. Through this immune learning based on memory, the unknown attack can be turned into a new known attack in the feature space of attacks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

NSIPRP Routing Protocol Based on AO2P:

In AO2P-based NSIPRP, a source discovers the route through the delivery of a routing request to its destination and the attack detection of candidate next node based on the normal model of selfs in the node and immune model. A node en-route from one normal node to another normal node will generate a pseudo node ID and a temporary MAC address. Once a route is built up, data is forwarded from the source to the destination based on the pseudo IDs and the immune detection mechanism. Once a compromised node is detected with the immunization on the normal model, the node should be under some attacks and will be repaired by recovering the compromised node after eliminating the attacks.

This section gives the details on AO2P-based routing discovery with immunity. Other issues, such as immune detection and secure data delivery with immunity, are addressed in section 4. Once a source needs to find the route to its destination, it first generates a pseudo ID and a temporary MAC address for itself through a globally defined hash function using its position and the current time as the inputs [1]. Because of the space-time unique identification, such a procedure makes the probability that two nodes involved in routing have the same ID and MAC address small and negligible.

The source then sends out a routing request (rreq) message. The rreq message carries the information needed for routing, such as the position of the destination and the source's pseudo ID. The neighboring nodes around the source, called receivers, should be detected by the native immune tiers of the receivers before the receivers receive the rreq. If a receiver is determined as a non-compromised one by the immune detection and the receiver is the destination, the connection between the source and the destination will be confirmed by more messages. If the receive is compromised, the receiver will be isolated by the immune tier so that the source will not send the rreq message to the compromised node until the node has been repaired well. At the same time, another receiver will be checked to expand the route until the destination is found in the end. . If the receiver is a non-compromised one and is not the destination yet, the receiver will assign itself to a receiver class following the rules for classifying nodes based on the positions [1] and the immune detection against the attacks.

Each non-compromised receiver uses the hash function to generate a pseudo ID and a temporary MAC address. The inputs of the hash function are the receiver's position and the time it receives the rreq. If any receiver is compromised due to the collaborative attacks, the receiver will have no pseudo ID or temporary MAC so that the attacks on the receiver can be easier to detect and eliminated than those with the pseudo ID and the temporary MAC. The receivers then contend for the wireless channel to send out hop reply (hrep) messages in a so-called rreq contention phase [1].

The receiver that has successfully sent out the hrep will be the next hop. If the receiver is compromised because of the attacks, the immune tier of the receiver will send back an attack message to the source, as shown in Fig. 2. After the compromised receiver has been repaired, the immune tier of the receiver will send back a repaired message to the source so that the source can send the rreq message to the repaired receiver again.

On receiving the hrep, the source replies with a message of confirming (cnfm), and then the next hop of thesource replies to this message with an ack. Upon receiving the ack, the source saves the pseudo ID and the temporary MAC address of the next hop in its routing table. After receiving the cnfm, the next-hop receiver becomes a sender, which is defined as the source or an intermediate node to forward the rreq message. Once the sender receives a hrep, it couples the pseudo ID and the temporary MAC address of its next hop with those of its previous hop and saves the pairs in the routing table. The searching of the next hop is repeated until the destination receives the rreq. After receiving the cnfm from its previous hop, the destination sends a routing reply (rrep) message through the reverse path to the source.

Themessage flow in AO2P-based NSIPRP routing discovery is shown in Fig. 2, and the frames for important control messages.A route discovery failure will occur when a sender cannot find a legitimate next hop. Routing discovery failure may also be caused due to destination mobility and/or the collaborative attacks. In these cases, a routing discovery failure report will be sent back to the source. The source will start a new route search based on the destination's most updated position after the compromised nodes in the route have been repaired.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

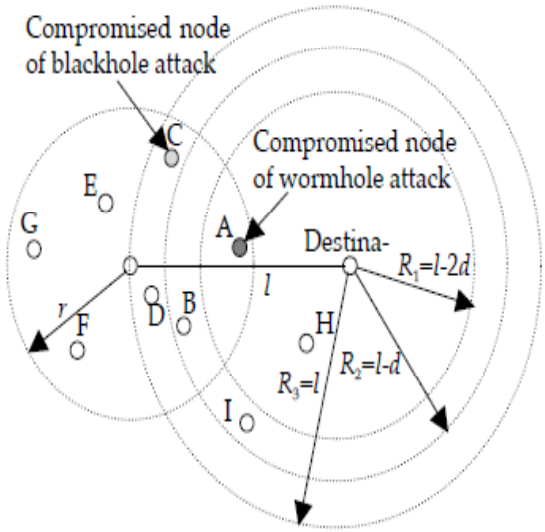


Fig. Classifying nodes based on the positions and the immune detection against the attacks.

SIMULATION RESULT:

The simulation scenario is a network covering an area of , where a number of nodes are uniformly deployed. The transmission range for the ad hoc channel is 250m. The receivers are divided into 4 classes according to the rules. To avoid disturbances from the warm-up period, the first 2 seconds of the simulation results were excluded. NS2 is used as the simulator, because it has the well-developed mobile Ad-hoc network model. The almost same simulation parameters are used in the NSIPRP-based network as that of the AO2P-based network , the varying probability of a routing failure in NSIPRP as some neighboring receivers of the mobile ad hoc network are attacked and immunized.

The x-axis is the reaction time of the simulation, and the collaborative attacks are of the wormhole attacks and the blackhole attacks. In the simulation, the probability of routing failure in the normal mobile ad hoc network is kept the lowest, i.e. 0.02. Unfortunately, the collaborative attacks obviously increase the probability of routing failure in the network, and then the probability becomes 1 especially when the wormhole attacks spread all over the network. Though the regular IDS approach can detect the known blackhole attack and decrease the probability of routing failure in the attacked network from 3s to 6s , the probability of routing failure increases obviously from 6s to 10s because the spread of the unknown wormhole attacks conquered the whole network in the end.

At the time that all the nodes of the network are infected by the wormhole attacks, the private information on the nodes is easier to steal by the attackers even if the information is encrypted. Fortunately, the NSIPRP-based immune network can work strongly against the collaborative attacks and decrease the probability of routing failure in the attacked network to the normal value. compares the simulated delivery ratio in the networks on the different conditions of the collaborative attacks and the NSIPRP-based immunization.

It shows that, generally, the normal AO2P-based mobile ad hoc network has the highest delivery ratio as it is not attacked at all. The attacked AO2P-based network without any defensive mechanism has the lowest delivery ratio. The regular IDS approach can deal with the known attack and increase the delivery ratio from 3l to 6s. But some unknownattacks can conquer the AO2P-based network with IDS, and the delivery ratio decreases to the lowest in the end. The NSIPRP-based immunization approach iseffective for the mobile ad hoc network against the collaborative attacks, and the delivery ratio increases to the highest after the immunization is activated.

CONCLUSIONS :

Some important properties and mechanisms of cooperative immunization were proposed to defend the ad hoc network under such collaborative attacks as the blackhole attacks and the wormhole attacks. New tritier cooperative immunization- based framework was designed to detect and recognize the collaborative attacks in mobile ad hoc networks such as WiMAX networks. The performance of the proposed framework was analyzed in terms of the PDRs, the throughput, the traffic overhead, and the responsiveness of the system. The experimental results confirm the effectiveness of the proposed cooperative immune model in detecting and mitigating these collaborative attacks from disrupting . the protected mobile ad hoc networks such as WiMAX networks.

REFERENCES:

1. Bhargava B, Zhang Y, Idika N, et al. Collaborative attacks in WiMAX networks. Security and Communication Networks 2009; 2(5): 373–391.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

2.Bhargava B, Oliveira R, Zhang Y, et al. Addressing collaborative attacks and defense in ad hoc wireless networks. In 29th IEEE International Workshops on Distributed Computing Systems. 2009; 447–450.

3.Sukwong O, Kim HS, Hoe JC. Commercial antivirus software effectiveness: an empirical study. IEEE Computer 2011; 44(3): 63–70.

4.Zhou JS, Chen Z, Jiang W. Probability based IDS towards secure WMN. In 2010 2nd International Workshop on -Intelligent Systems and Applications. 2010; 1–4.

5.Garcia-Osorio A, Loo-Yau JR, Reynoso- Hernandez JA. A GaN class-F PA with 600MHz bandwidth and 62.5% of PAE suitable for WiMAX frequencies. In 2010 IEEE International Microwave Workshop Series on RF Front-ends for Software Defined and Cognitive Radio Solutions (IMWS). 2010; 1–4.

6.Moore D, Paxson V, Savage S, et al. Inside the slammer worm. IEEE Security and Privacy 2003; 1(4): 33–39.

7.Schuba CL, Krsul IV, Kuhn MG, et al. Analysis of a denial of service attack on TCP. In IEEE Symposium on Security and Privacy. 1997; 208–223.

8.Cheung S, Lindqvist U, Fong M. Modeling multistep cyber attacks for scenario recognition. In DARPA Information Survivability Conference and Exposition, Vol. 1, 2003; 284–292.

9.J. Yang, P. Ning, and X.S. Wang, et al, "CARDS: A distributed system for detecting coordinated attacks," Proceedings of IFIP TC11 16th Annual Working Conference on Information Security, pp. 171-180, 2000.

10.A. Hussain, J. Heidemann, and C. Papadopoulos, "COSSACK: coordinated suppression of simultaneous attacks," Proceedings of DISCEX, pp. 2-13, 2003.

11.D. Ourston, S. Matzner, and W. Stump, et al, "Coordinated internet attacks: responding to attack complexity," Journal of Computer Security, vol. 12, no. 2, pp. 165-190, April 2004.

12. F. Cuppens and A. Miege, "Alert correlation in a cooperative intrusion detection framework," Proceedings of IEEE Symposium on Security and Privacy, pp. 202-215, 2002.

13.W. Lin, L. Xiang, and D. Pao, et al, "Collaborative Distributed Intrusion Detection System," Proceedings of 2nd International Conference on Future Generation Communication and Networking, pp. 172-177, 2008.

14.W. Yu-Sung, B. Foo, and Y. Mei, et al, "Collaborative intrusion detection system (CIDS): a framework for accurate and efficient IDS," Proceedings of Computer Security Applications Conference, pp. 234-244, 2003.

15. Mohamed YA, Abdullah AB. Immune inspired frame work for ad hoc network security. In Proceedings of2009 IEEE International Conference on Control and Automation. 2009; 297–302.

16.Atakan B, Gulbahar B, Akan OB. Immune system inspired evolutionary opportunistic spectrum access in cognitive radio ad hoc networks. In Proceedings of 2010 The 9th IFIP Annual Mediterranean Ad Hoc Networking Workshop. 2010; 1–8.

17. Matzinger P. The danger model: a renewed sense of self. Science 2002; 12: 301–305.