International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 175-184, 2018, ISSN:-2319–8656

Intrusion Detection against DDoS Attack in WiMAX Network by Artificial Immune System

Mehrafrooz Reyhani
Department of Computer Science, Yazd Branch, Islamic Azad University, Yazd, Iran

Vahid Ayatollahitafti*
Department of Computer Science,Taft Branch, Islamic Azad University,Taft,Yazd, Iran

Mohsen Sardari Zarchi
Department of Computer Engineering, Meybod University, Meybod
Iran

Abstract: IEEE 802.16, known as WiMax, is at the top of communication technology because it is gaining a great position in the wireless networks. In this paper, an intrusion detection system for DDOS attacks diagnosis is proposed, inspired by artificial immune system. Since the detection unit on all subscriber stations in the network is WIMAX, proposed system is a fully distributed system. A risk theory is used for antigens detection in attack time. The proposed system decreases the attack effects and increases network performance. Results of simulation show that the proposed system improves negative selection time, detection Precision, and ability to identify new attacks compared to the similar algorithm.

Keywords: **WIMAX network, Artificial Immune System, DDOS Attack**

1. INTRODUCTION

Computer networks are changing and developing very quickly either in architecture context or software context of the network and these changes affect the network traffic. Therefore, the examination of the network traffic has always been discussed by researchers. WiMAX network is very dynamic and it is possible that the topology between stations be different from physical network, also the shared files can be replaced according to the topology of wireless network. Therefore, traffic in WiMAX network can be examined from different aspects such as, the distribution of packet entrance in time unit, the interval between packet entrance and the distribution of packet size. If the number of these packets exceeds the threshold value, network resources will be saturated, because the stations in WiMAX network leave the network or join it in anytime[1,2]. Therefore, they will be exposed to DDoS attacks and such behaviors should be detected and prevented. In order to prevent, detect, encounter and stop attack, security should be recognized and created over the network in the first stage. The first security level is to prevent intrusion and intrusion detection system is the second defensive line. The main strategy to solve security problem in WiMAX network is to use intrusion detection system. By using these strategies, it is possible to detect suspicious ways and potential attacks. As current systems are continuously changing and the strategies to intrude them are also gradually changing, it is essential that intrusion detection system be dynamic over time.

Two noticeable factors in vulnerability of WiMAX network are the flooding sent of message and its decentralized nature [3]. If DDoS attack is managed, it can be controlled in other wireless networks. As DDoS attack contains a large number of distributed machines, the development of defensive nodes would be effective in discovering DDoS attack. Collaborative discovery requires that heterogeneous stations be adhered and it guarantees high scalability and security against attacks [4,5].

Considering the main features of distributed systems and also examining the different mechanisms of human immune system can reveal some similarities between these two seemingly different contexts. Regarding these similarities, we are inspired by human immune system to identify effective intrusion in distributed systems. In the suggested system the combination of artificial immune system algorithms are used. This system follows its operation in several levels with heterogeneous functions of stations.

The rest of this paper is organized as follows. In section (2), we describe the intrusion detection system which is related to this context and we briefly introduce intrusion detection by inspired from artificial immune system. In section (3), includes a brief analysis of suggested intrusion detection system, the results and details of our dataset. Finally in section (4), the paper is concluded with a discussion of our proposed intrusion detection system and artificial immune system.

2. REVIEW OF LITARETURE

The majority of researches examining attacks just focus on one system but the attacker's purpose is to sabotage several systems. Since the suggested system is based on human immune system, in this section we outline previous studies about the intrusion detection system of WiMAX network and also researches that exploit human immune system to secure computer networks.

INTCD [6] is a distributed system based on neural networks for detecting network traffic anomalies and for dynamically modifying the network resource access policies. Initial data of network traffic is examined and any suspicious behavior is discovered. One of the advantages of this system is flexibility but before doing anything, some data should be thought to this system.

DD-police [7] protects wireless network against DoS (Denial of Service) attack. In this model, stations supervise their neighbors' traffic. If a node receives a lot of requests from its neighbor, this neighbor will be identified as a suspicious node. Scalability and frequency of sending neighbors' list are two factors that should be mentioned in this model. In wireless network with its high dynamic nature, nodes leave and join a lot, and also increase in the frequency of neighbors' list raises the system's overload.

In the context of exploiting the features of human immune system for the security of computer networks, Forrest performed the first researches to discriminate between self and nonself in network artificial immune system. Then Hofmeyr [8] designed an artificial immune system called ARTIS. This system is not very efficient because collaboration and information exchange among nodes is not considered and intrusion detection is done separately in each computer.

LISYS [9] is one of the first structures for artificial immune systems that is designed for a simple local network and can learn network traffic and identified anomaly traffic.

CVIS [10] has some characteristics such as analyzing the discovered virus, repairing defective files and spreading the results of analysis to other local systems. Although CVIS operates in a distributed environment using the autonomous factors but scalability is its cliché problem.

CDIS [11] is also designed in artificial immune system to detect computer viruses. CDIS is a developed form of LISYS and both have the same base. The life cycle of detectors is also same. In the both of them, detectors (antibodies) are randomly produced in both. This system can detect viruses and network intrusions. CDIS is a multilayer and distributed computational immune system. One of the problems of CDIS structure is that it only analyzes and examines one packet in anytime.

The purpose of Cfengine [12] system is to automatically configure large number of systems on heterogeneous nodes. Furthermore, as long as a new discordance does not happen, the intrusion detection system is passive. In order to increase scalability, Cfengine intrusion detection system updates the average of system efficiency, the number of each service input and output connection and packet characteristic. Results of Cfengine show that danger signal potentially affects false positive rate and also memory detectors improve detection rate.

3- THE PROPOSED INTRUSION DETECTION SYSTEM

Since the proposed system contains new ideas and a combination of different algorithms are used to developed purposes, we will investigate this system from three different aspects: intrusion detection system, WiMAX network and artificial immune system.

3.1 INTRUSION DETECTION SYSTEM

As the proposed intrusion detection system is located in all subscriber station, system announces the existence of attack or intrusion to

other Base station by means of distributive BS warning. Consequently the stated system discovers the network intrusions by cooperation between SS and BS.

Intrusion detection system can be divided into two different groups: network intrusion detection system (NIDS) and host intrusion detection system (HIDS) [13,14].

NIDS is installed on the network's gateway and examines the traffic of the network from which it passes. Since BS in WiMAX network plays the role of gateway and also the role of decided in distinguishing anomaly traffic from normal traffic, the BS sends attack strategy to other BSs after identifying and proving attack.

HIDS performs on different nodes based on collecting network traffic information. These pieces of information are separately analyzed in each node and the results are used to immune the activities of the aforementioned node. Obviously the proposed intrusion detection system is located on all SS so this system performs distributive. The results, informs other nodes in WiMAX network of the existence attacker node.

To detect intrusion, the algorithms of artificial immune system such as negative selection [15] and clonal selection [16] are used. In fact, new and unknown attacks are detected. Anomaly traffic and normal traffic are distinguished using danger theory. Therefore, the proposed system is formed by the process of combining two methods. In the training phase use anomaly-based intrusion detection and in the test phase utilize signature-based intrusion detection.

By saturation of network resources in a short time and prediction of attack possibility, the node (BS and SS) in the suggested intrusion detection system warns its BSs to confront attacks. Therefore, on surrounding BS become aware of possible attack. Invaded nodes would be suspended since they are not resistant against attack and they are protected to some extent. This system has an active attitude by detecting and announcing SS and BS new behaviors.

It should be mentioned that SSs perform intrusion detection continuously but BSs would be active just by sending the Stress message from SSs.

3.2 ARTIFICIAL IMMUNE ALGORITHM

Since human immune system performs actively and distributively, artificial immune system algorithms are extremely used in proposed system to develop purpose. Here major features of human immune system are inspected to detect intrusion and how it reacts against intrusions. Then its application in WiMAX network to confront DDoS attack will be mentioned.

In the suggested system negative selection algorithm is used in training phase and its function is as follows:

Network normal traffic which contains WiMAX network packets is captured by TFN2K monitoring tools. Then it considered as a self-dataset. After that some detectors(immature detectors) are produced by random Gaussian function and by comparing these two datasets, any detectors that do not correspond to network normal traffic will be added to the detectors' list as none self-detector(mature detectors). In this stage, the number of detectors is investigated. If this number increases, the accuracy of detection goes up and computational overload increases too.

Algorithm 1. Negative selection method in training phase

Input: selfdata

Output: detectors

Use KDD dataset for normal traffic

W_{nd}: WiMAX normal dataset

W_{ad}: WiMAX abnormal dataset (detector dataset)

D: detector

D_{th}: Threshold of detector

1: **while** number of d less than D_{th}

2: d← create immature detector with uniform Gaussian random function

3: **if** W_{nd} contains d **then**

4: drop d

5: **else**

6: d insert into W_{ad}

7: **end if**

8: **end while**

After receiving each WiMAX packet, the information will be added to template. Then the size of bandwidth occupation will be examined. If it does not reach to the default threshold(70%), the template will be faded out of existence and a new template will be made.

Otherwise, the possibility of attack occurrence will be announced to connect BSs and then SS after making sure of the existence of each BS sends the template of possible attack (the structure of antigen DNA) to each BS. In this stage, SS announces the possibility of attack occurrence and distinguishes between abnormal traffic and normal traffic. SS will be suspended in a definite time span to prevent the reception of any packet or message. When this time span ends, SS will return to its initial state.

BS announce its existence to SS by receiving the possibility of attack occurrence and after receiving the template of possible attack compares that to its nonself dataset. If the template conforms to each detector, BS broadcasts it to other BSs as a detector. Then BS creates conformed detectors once again, increases their affinity and if detectors aren't conformed, BS will make them older. In either way BS examines detectors' affinity in order to change its main structure.

According to the number of conformities, detectors' situation changes from mature stage to active stage and from active stage to memory stage. In next step each detector's beneficial life time along with its kind is inspected. As each kind of detector has a definite life time, those detectors whose life time is ended are deleted from detectors dataset.

Genetic algorithm is used to improve detectors in the proposed system. This algorithm also causes variety in nonself templates in active stage, in a way that based on clonal selection algorithm, those cells that identify detector grow and those cells that are not able to identify detector die.

As SS and BS operate in a collaborative and parallel manner, SS's and BS's function are separately inspected.

Algorithm 2. Subscriber station(mobile node) Function in test phase

Input:anomaly wimax traffic

Output: template message

W_p: WiMAX Packet

BW_d: percentage of Subscriber station Bandwidth depletion

BW_{th}: Threshold of Subscriber station Bandwidth depletion

01: **While** SS is in active mode

02: T← receive features of new W_p

03: **if** $BW_d \geq BW_{th}$ **then**

04: forwards msg-stress along connected Base Station

05: **else**

06: Drop T

07: **end if**

08: **if** received msg-sressreply **then**

09: forwards T to certain Base Station

10: stand in suspend mode for time span

11: **end if**

12: **end while**

Algorithm 3. Base Station Function in test phase

Input:template message

Output: detector

T_a: Template of attack

T_c: number of conformity with Ta

T_{ttl}: time to live for every detectors

01: **while** Base Station is in active mode

02: T← receive W_p

03: **if** W_p.Type is msg_stress **then**

04: forwards msg_stressreply along subscriber station

05: **end if**

06: T_a← received msg_template

07: **if** W_{ad} contains T_a **then**

08: increment T_c

09: set T_{ttl} to zero

10: update W_{ad} with T_a

11: forward T_a along every Base Station in network

12: Run GA .Algorithm on W_{ad}

13: **end if**

14: **end while**

4. PERFORMANCE EVALUATION

We implemented intrusion detection system in WiMAX network used OPNET simulator 14.5. This version of simulator is first version that embedded 802.16 standards. Radio source in WiMAX network are consisted by time/frequency slices. The number of slices in downlink depends on related system bandwidth, frame period, downlink/uplink rate, permutations under vector (AMC, FUSC, PUSC), and protocol header (FCH, maps, preamble).

4.1 SIMULATION DATA PRELIMINARIES

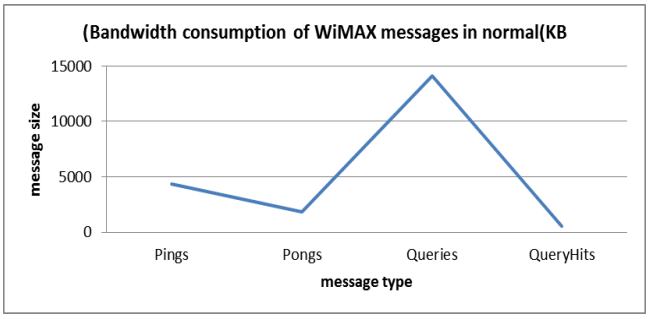
Three subnets with different numbers of nodes were used in simulation scenario that is WiMAX network with metroethernet structure. The connection between subnets is done with third layer switch, and VLAN is used to prioritize to traffic. To increase security in WiMAX network, server connection and relation between BS and metroethernet structure were considered. In this simulation, number of production packets was considered 50 packets in an hour and 300 seconds for production time. Transmission packets used IP/UDP protocols. In simulation scenario WiMAX network with metroethernet structure, number of mobile nodes in each all or even in each subnet was considered to study varios factors and their changes. System bandwidth is 2.5GHz, TDD frame period in WiMAX is equal to 5ms and ratio of downlink to uplink is . PUSC was considered in simulation. For the simplicity, protocol header consists of two fields. Number of slices in each TDD sub frame equals to NS=450. The parameters are shown in table 1.

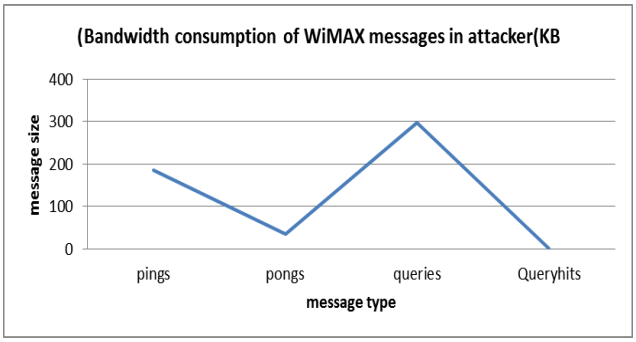
Table 1. Simulation parameters

Parameters	value
Base frequency	2.5GHz
Duplexing mode	TDD
System bandwidth	5Mbps
Propagation model	Two ray ground
Cell radius	50m
DL/UL ratio	3:2(27:18 OFDM symbols)
Frame length	5ms
PHY	OFDM
DL permutation zone	PUSC
MAC PDU size	Variable
Inter-arrival between frames	120ms
Simulation time	300s
Number of detector	75

In the early stage of simulation, the type of WiMAX message is used to form attack template. But as maximum of messages is related to Query message, an almost similar template is achieved in the definite time span and in order to prove that. Transmitted messages in WiMAX network are examined in three conditions: normal, attacker node and victim node.

When DDOS attack happened, the used bandwidth of each WiMAX messages was examined and according to various experiments on victim stations and attacker stations, the maximum consumption was related to Query message. Figure 1 proves this claim.





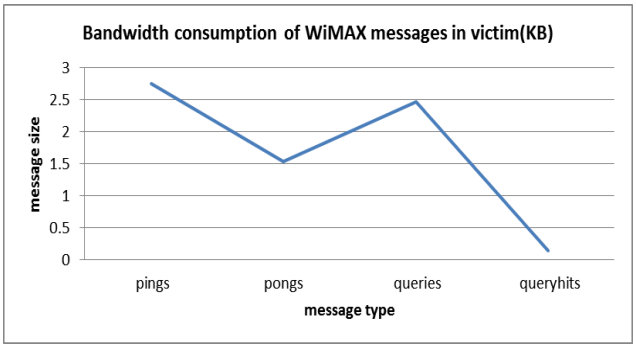
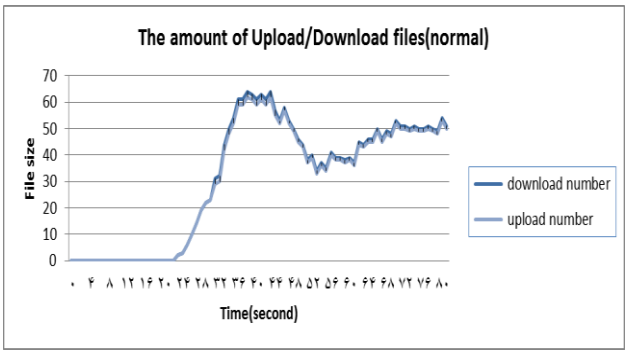
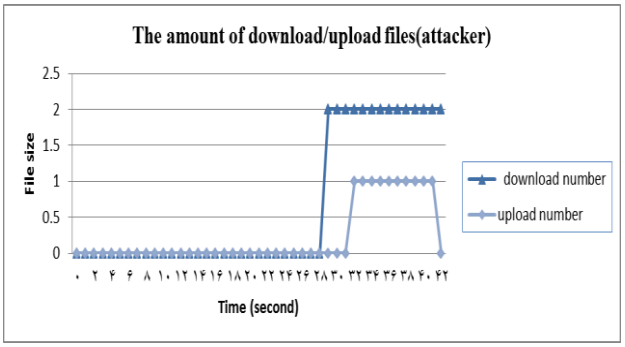


Fig.1. Bandwidth consumption of WiMAX messages in normal condition, attacker, victim.

The number of shared files is evaluated in both normal and attack conditions. In normal condition, the amount of files download and upload has approximately been equal but in attack condition the amount of download has been minimized. This is shown in figures 2. The real network in normal condition, maximum traffic is related to download shared files.





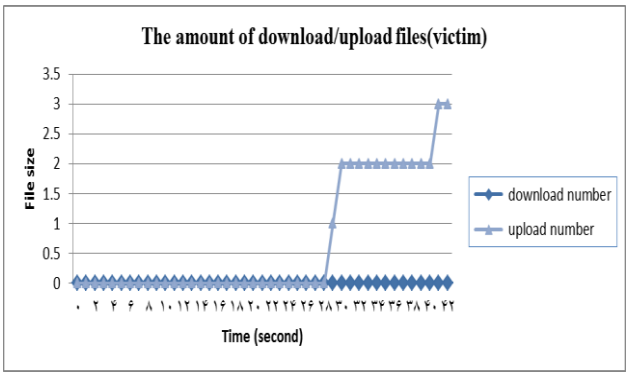


Fig.2. The amount of downloaded and uploaded files (a) normal condition (b) attack condition for attacker (c) attack condition for victim

In next step, we have formed template by factors such as source IP address, destination IP address and average of time interval between consecutive two messages. As the majority of messages are Query, recording message type is something extra. When the source IP address and the time of message sending are equal, attacker node can be identified and DDOS attack can be announced by examining the source IP address and time interval which is passed to send the packet to destination. In fact, if the IP address of messages and the time interval which is passed until packets get to destination are equal and the consumption bandwidth exceeds threshold, DDoS attack has happened.

4.2. SIMULATION RESULTS ANALYSIS

The efficiency of proposed system is analyzed based on the following criteria:

- Negative selection time

- Detection Precision
- Ability to identify new attacks

Negative selection time: Some immature detectors are produced by random Gaussian function and this dataset compares with WiMAX normal dataset. If any detectors do not match with normal traffic template, it will be added to the mature detectors' list. Output of training file is a mature detectors' dataset. The small amount of dataset used in this simulation and also the dataset which has been chosen for conformity decreases the time of negative selection in comparison to LISYS algorithm. Figure 3 shows time of negative selection in proportion to the size of training file.

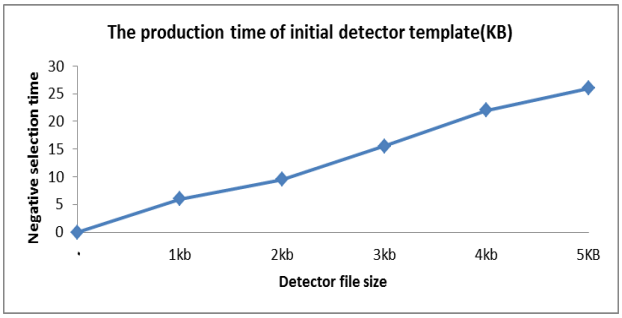


Fig.3. The production time of initial detector template.

Figure 4 Shows the time of negative selection in proportion to the number of detectors. By increasing number of mature detectors, negative selection time will be increase too but, detection precision is optimized. Because of using genetic algorithm, the time of negative selection is more beneficial than LISYS algorithm.

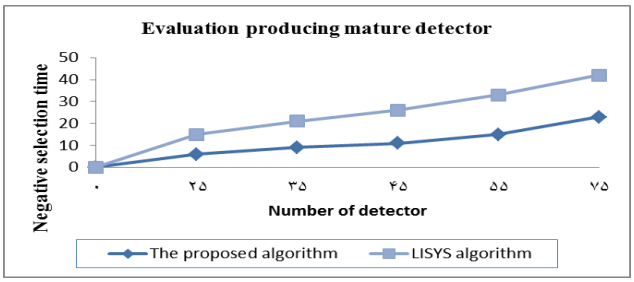


Fig.4. The production time of mature detector.

Detection Precision: In order to increase detection precision, false positive should be reduced.

These parameters include:

- The number of detectors
- The specificity of detection (the r parameters of bit matching algorithm)
- The crossover and mutation operators for genetic algorithm.

We also look at which parameters appears most important for minimizing false positives, as well as how maximizing percentage of detecting intrusions. The percentage of attack detection will be measured by proportion of discovered attack occurrences to all attack occurrences.

In fact «false positive is the sending of alarm message by intrusion detection system in the time that attack has not happened».

The proposed system is adopted to describe the tradeoff between the detection rate and false positive rate. Therefore, we evaluate the best attitude coherent to these factors for yielding optimum resolves.

a. number of detectors

To study the effect of mature detectors on the percentage of attack discovery and false positive, the parameter of activation discovery is considered 6, crossover operator 0.4 and mutation operator 0.005. These two factors are evaluated by the change in the number of detectors in the number of different conformity bits. Through increase in the number of detectors, the percentage of attack discovery goes up on the one side and the false positive increases on the other side. In a way that in all the forms of conformity bit, 75 detectors show the most efficient response for detecting attack. But due to computation over load, the number detectors are commonly not very high. In LISYS algorithm, the number of detectors is 100. Figure 5 proves this.

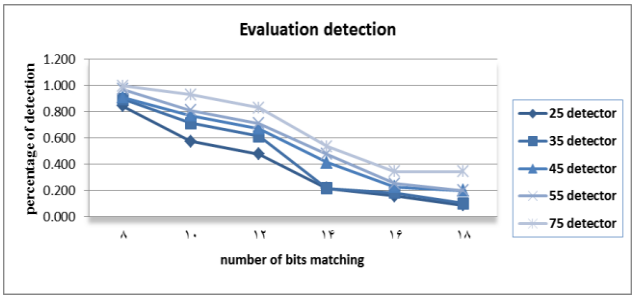
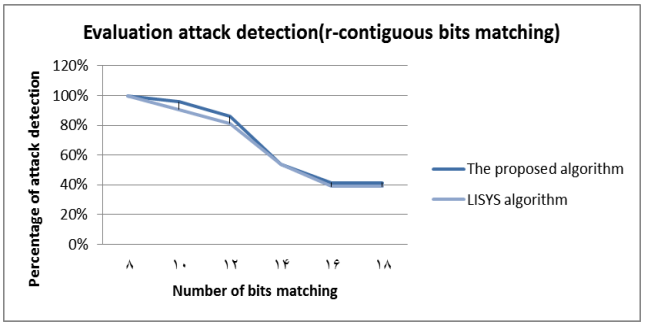


Fig. 5. Evaluation detection with different number of detector

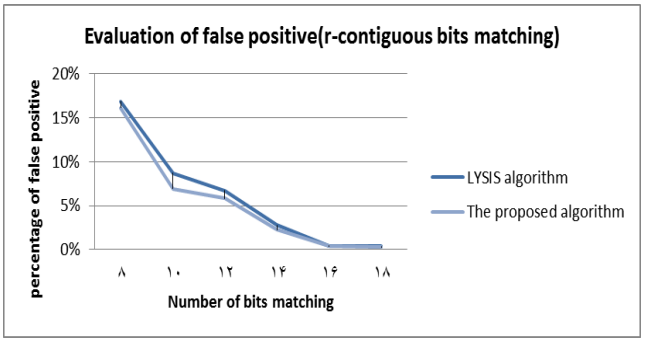
b. parameters of bit matching algorithm

Some detectors in this system usually implement as strings, whose function is to classify new strings as normal or abnormal by matching them in some forms. The perfect matching is rare in the immune system. So, we use a partial matching rule is known as r-contiguous bits matching. Under this rule, two strings match if they are identical in at least r contiguous locations.

Our observations in figure 6 show that immune system as inspiration for detecting intrusion is the best approaches. In particular, the r-contiguous bits matching rule is proposed in LISYS and we use it for our system. To study the effect of mature detectors on the percentage of attack discovery and false positive, the parameter of activation discovery is considered 6, crossover operator 0.4 and mutation operator 0.005. These two factors are evaluated by the change in the number of detectors in the number of different conformity bits. The number of strings a detector matches increases exponentially as the value of r decreases. For example, 8 conformity bits is the best resolve for attack detection rate but is the worst result for false positive rate. After checking these factors, we elect 8 conformity bits and LISYS algorithm elect the number, too.



(a)



(b)

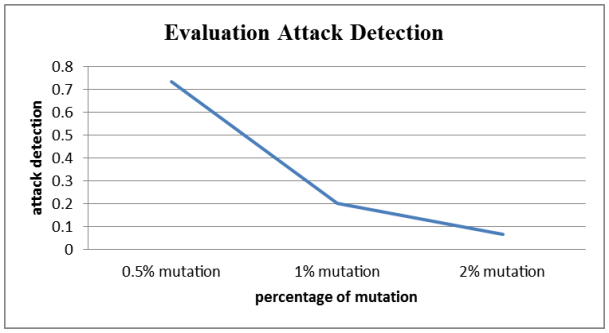
Fig.6. Evaluation attack Detection and Evaluation false positive

C. Crossover and mutation parameters

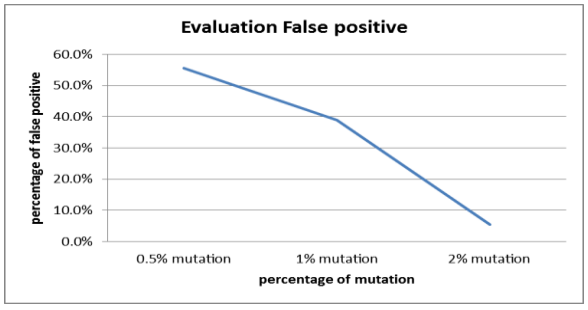
As 100 attacks are discovered, generation production happens once, but with occurrence of each attack, homeostasis process is defined, in other words the detectors that should be thrown away or remain in the detectors set are defined.

In this condition the number of detectors is considered in the best state which is 75. The highest detection percentage is found by the number of bit conformity and activation threshold and then mutation rate is examined and finally the best mutation rate is computed for the highest discovery percentage.

As 73% of the best attack detection responses have the mutation rate of 0.005 and also in the examination of false positive, 56% of the lowest false positive is related to mutation rate of 0.005, therefore in the suggested system the same mutation rate is used.



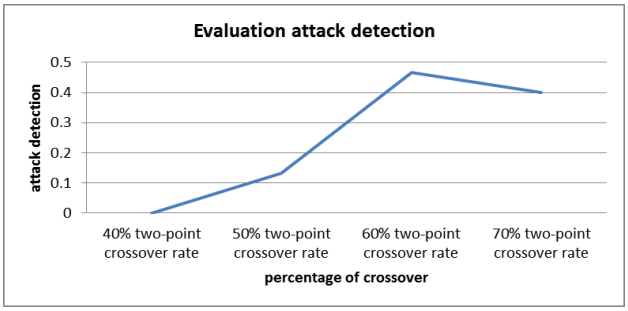
(a)



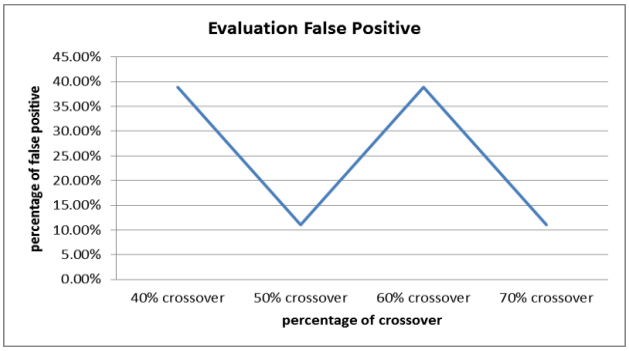
(b)

Fig.7. Evaluation attack detection and evaluation false positive

In this condition the number of detectors is considered in the best state which is 75. The highest detection percentage is found by 12 conformity bits, activation threshold and then crossover rate is examined and finally the best crossover rate is computed for the highest discovery percentage and the lowest false positives percentage. As 47% of the best attack detection responses have the crossover rate of 0.6 and also in the examination of false positive, the lowest false positive is related to crossover rate of 0.4 and 0.6, therefore in the suggested system the 0.6 crossover is elected.



(a)



(b)

Fig.8. Evaluation attack detection and evaluation false positive

Ability to identify new attacks: As the training phase of this system is performed on all nodes and also in the stage of BS checking, with the attack detection, its pattern is sent to other BSs, therefore there is a high variation in patterns and consequently the suggested system has the ability to discover new attacks. The new attack template rate measures the ratio of number new attack template that before we do not have this template to all attack traffic

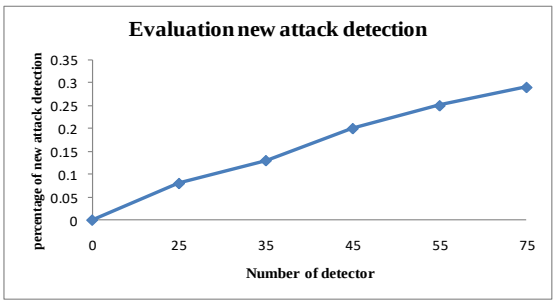


Fig.9. The percentage of new attack detection

5. CONCLUSION

Since establishing security in distribution networks is complicated to reach maximum security and detect portable attacks, it is important to use advantages of different methods of penetration detection. In a way that penetration detection in proposed system, use a combination of detection approach based on normal traffic and attack traffic. To analyze the proposed algorithm, we detain WiMAX message data by TCPDUMP tools. In each detection using genetic algorithm, a new generation is established that is added to antigen set, indeed, we detect new attack template that increases the ability of this system and by decreasing false positive, increased the accuracy of attack detection. The proposed system in this paper, after distinguishing the attack using policies minimize the attack influences and optimize the operation of system. In addition to that proposed system, collaboration between nodes and way of using artificial immune system algorithms is studied. In following papers, by using the operation of regulating T cells, normal nonself templates to decrease false negative. Also, by considering vaccine process in detection virus, it can be announced to detect system that there is an attack and needed reactions should be shown and make some detectors for detection. As in this study, WiMAX has been used but in WiMAX network, the second version is used in research and yet it is not used practically, and this version has so many parameters such as encryption with public key and Kerberos authentication algorithms, so we can obtain desirable results by using proposed algorithms in network.

REFERENCES

[1]D. Pareit, I. Moerman, P. Demester, The history of WiMAX: A complete survey of the evolution in certification and standardization for IEEE 802.16 and WiMAX, IEEE Communication, vol. 14, no. 4(2012): 1183–1211.

[2]Y. Zou, J. Zhu, X.Wang, L. Hanzo, A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends, Vol. 104, No. 9, (2016): 1123-1161.

[3]P. Jadon, Detection and Mitigation of Flooding Attack in WIMAX Network, International Journal of Current Trends in Engineering & Technology, Volume: 02, Issue: 03(2016): 823-828.

[4]G.Oikonomou, P. Reiher, M. Robinson, and J. Mirkovic. "A framework for collaborative DDOS defense." *in Proceedings of the 2015 annual computer security applications conference*, (2015): 33-42.

[5]Ch. Zhang, Zh. Cai, W.Chen, X.Luo, J. Yin, Flow level detection and filtering of low-rate DDoS, Computer Networks 56 (2014) : 3417–3431.

[6]Daniel SIMION, M.-F. U.. An Overview on WiMAX Security Weaknesses/Potential Solutions. *11th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania* , (2012): 110-117.

[7]M Alzaabi, K. D. SECURITY ALGORITHMS FOR WIMAX. *International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3* , (2013): 62-75.

[8]F. Esponda,S. Forrest and P. Helman. "A formal framework for positive and negative detection schemes." *IEEE Transactions on System, Man, and Cybernetics 34(1)*, (2014): 357–373.

[9]j. Balthrop, S. Forrest and M. Glickman. "Revisiting lisys: Parameters and normal behavior." *In CEC-2002: Proceedings of the Congress on Evolutionary Computing*, (2002).

[10] S. Stepney, R. Smith, J. Timmis, and A. Tyrrell. "Towards a conceptual framework for artificial immune systems." *In Proceeding of the 9rd International Conference on Artificial Immune Systems (ICARIS), LNCS 3239*, (2015): 53-64.

[11] P. Williams, K. Anchor, J. Bebo, G. Gunsch, and G. Lamont. "CDIS: Towards a computer immune system for detecting network intrusions." *In In RAID 2014, volume 2212*, (2014): 117–133.

[12] U. Aickelin, P. Bentley, S. Cayzer, J. Kim and J. McLeod. "Danger Theory: The Link between Artificial Immune Systems and Intrusion Detection Systems." *Proceedings 2nd International Conference on Artificial Immune Systems*,(2013): 147-155.

[13] P. Jadon, Detection and Mitigation of Flooding Attack in WIMAX Network, International Journal of Current Trends in Engineering & Technology, Volume: 02, Issue: 03(2016): 823-828.

[14] G.Oikonomou, P. Reiher, M. Robinson, and J. Mirkovic. "A framework for collaborative DDOS defense." *in Proceedings of the 2015 annual computer security applications conference*, (2015): 33-42.

[15] S. Singh. "Anomaly detection using negative selection based on the r-contiguous matching rule." *in Proceedings of the 1st International Conference on Artificial Immune Systems (ICARIS'-15)*, (2015): 99-106.

[16] W. Zhang, J. Lin, H. Jing, and Q. Zhang. " A Novel Hybrid Clonal Selection Algorithm with Combinatorial Recombination and Modified Hyper mutation Operators for Global Optimization", Computational Intelligence and Neuroscience Volume 2016, Article ID 6204728(2016): 1003-1016.