An Entropy Based Approach for DDoS Attack Detection in IEEE 802.16 Based Networks

Maryam Shojaei, Naser Movahhedinia, and Behrouz Tork Ladani

Department of Computer Engineering, University of Isfahan Hezarjarib, Isfahan 81746, Iran
{m_shojaei,naserm,ladani}@eng.ui.ac.ir

Abstract. Distributed denial of service attacks are great security threats to computer networks, especially to large scale networks such as WiMAX. Detecting this kind of attack is not as easy as some other attacks, because the traffic created by attack is too similar to the traffic of the network in the normal case. So in this paper a novel framework is proposed to detect DDoS attack in IEEE802.16-based networks efficiently. The key idea of the proposed method is to exploit some statistical features of the incoming traffic. In fact we design a system in which some entropy-based features of the traffic are analyzed. Based on these features we decide whether the attack has occurred or not. Previous works have all focused on the entropy of IP address of the incoming packets, while in this system we have comprehensively considered some other entropy-based features which help a lot in detecting the attack rather than just considering the entropy of the incoming IP addresses. Also in the proposed method we have tried to exploit the long range dependency of the traffic to detect the attack. The simulation results show that the proposed method can detect DDoS attacks efficiently.

Keywords: WiMAX, DDoS attack, Entropy, Initial network entry, RNG-REQ Message.

1 Introduction

The WiMAX technology which is based on IEEE 802.16 may use radio transmission for high speed direct access to internet. Due to high bit rate and QoS support, WiMAX networks are able to offer multimedia services such as voice and video streaming and instant data transfers. Today Mobile WiMAX is one of the wireless broadband standards capable of providing the quadruple play technologies data, voice, video and mobility using a single network. Although many solutions have been presented for analyzing and detecting DDoS attacks, but still this threat is an important security problem for these networks [1,2,3]. Traditional wireless technologies such as 2.5G cellular networks are not exposed to DDoS attack since they are mainly based on circuit switching. However, with emergence of broadband wireless services like Mobile WiMAX system that are based on packet switching, cellular networks are no more safe against DDoS attacks [4,5,6]. In [1,7], Nasreldin, et al. studied the security vulnerabilities of IEEE 802.16 and categorized the threats as solved and unsolved ones. However interrupt attacks, such as DoS attacks, in which

T. Iwata and M. Nishigaki (Eds.): IWSEC 2011, LNCS 7038, pp. 129–143, 2011.

an intruding entity blocks information sent from the source entity to the destination entity have not been discussed much, and since WiMAX is a rather recent technology, this vulnerability has not been deservedly studied yet. In the next section of this paper the previous works in similar networks such as internet and heavy traffic campus networks will be reviewed then in section 3 a reference model which is used to simulate an attacked network and its traffic, bandwidth allocation for ranging and vulnerability to DDoS attacks are described. Section 4 presents the network traffic model and the method employed for calculating entropy-based parameters. In section 5 WiMAX network simulations with the mentioned vulnerability and the evaluated statistical parameters in different condition are described. Finally we conclude our paper in section 6.

2 Related Works and Background

2.1 DDoS Attack in Similar Networks

Since DDoS attacks can make a server or base station to go out of service, lots of researches have been done on this attack. In this section some works which have been done in similar networks will be reviewed. The researchers have used entropy and distributions of traffic features to detect DDoS attack and have paid a lot of attention to it. As one of the recent investigations, in [8] Lee, et al. used cluster analysis to detect DDoS attack by selecting some parameters and features of the traffic which show anomalies in the traffic. They used 2000 DARPA Intrusion Detection Scenario data set and as a result they divided the data to 5 groups. By extracting some features of the traffic which includes entropy of source and destination IP address, entropy of source and destination port number, entropy of packet type, occurrence rate of packet type (ICMP, UDP, TCP SYN) and number of packets and clustering them in to 5 groups, they differentiated between the normal and attack traffic. Among the five phases of the DDoS attack, they could detect three phases. In [9] George, et al. extracted two types of features from the network traffic. One type is extracted from the header of the received packets and the other type includes some behavioral features which are extracted from the network traffic. The first type includes source and destination IP address, source and destination port number and flow size distribution. The second type includes the in- and out-degree of each active internal IP address inside the network under consideration. By using CMU, GA Tech, Internet2 and G`EANT data sets and calculating the correlation between the extracted features they showed that there is a strong relationship between port and address distributions while the degree distributions and flow size distribution are weakly correlated with each other and with the port/address distributions. The correlation between the port number and addresses distribution arises due to the underlying traffic templates. In [10], Shui and Wanlei calculated the entropy of flows at a router, if the router entropy is less than a given threshold, then an attack alarm is raised and then the routers on the path of the suspected flow will calculate the entropy rate of the suspected flow. If the entropy rates are the same or the difference is less than a given value, then the traffic is marked as attack traffic and the packets are discarded. In [11] Sumit and Sahoo also used entropy and entropy rate to model an anomaly detection system for DDoS

attacks in grid computing. In their proposed algorithm, first the entropy of the received packets is estimated. If the estimated entropy exceeds the threshold, then the entropy rate will also is calculated and compared with a threshold. If it is more than the specified limit, the traffic is recognized as the attack traffic.

2.2 DDoS Attack in WiMAX Networks

The Mobile WiMAX is a broadband wireless technology that some of its security vulnerabilities are not much explored [1]. In [4] Youngwook et al. exploited the unused most significant 64 bits of the 128-bit Cipher-based Message Authentication Code (CMAC) which is designed to provide the integrity of management message. They used DREG REQ message to extract SAI and use it to defend the Mobile WiMAX network against DDoS attack. In fact they proposed a method to defend the network against the DDoS attack.

Since it is assumed that high-volume attack traffic causes significant changes in the power spectral density of traffic and few works have been done in understanding the analysis capability provided by a set of entropy metrics in conjunction with one another, our proposed method analyzes the network traffic by extracting more effective features. Since WiMAX networks are new technology few works have been done in these networks, so there is no real data set to compare the achieved results with the results of a real attack.

3 DDoS Attack on WiMAX Network

In this section interrupt attacks on WiMAX Networks such as DoS attacks are studied in brief.

3.1 Reference Network Model

The Mobile WiMAX Reference Network Model (RNM) consists of Access Service Network (ASN) and Connectivity Service Network (CSN) as shown in Fig. 1[4]. Constituted of several BSs and an ASN Gateway (ASN-GW) ASN provides radio connectivity service for its mobile subscribers (MS) and CSN offers IP access service to a number of ASN-GWs. A BS provides direct radio access to the MSs in its cell and ASN GW connects the BSs in its paging group to the CSN. (The ASN coordinates traffic across multiple Base Transceiver Stations (BTS) and supports security, handoffs and Quality of Service (QoS). Typically the ASN includes numerous BTSs with one or more ASN gateways. The ASN manages radio resources, MS access, mobility, security and QoS. It acts as a relay for the CSN for IP address allocation and AAA functions. The ASN gateway hosts the Mobile IP Foreign Agent (FA). The CSN performs core network functions, including policy and admission control, IP address allocation, billing and settlement. It hosts the Mobile IP Home Agent (HA), the IP and AAA servers, and PSTN and VoIP gateways. The CSN is also responsible for internetworking with non-WiMAX networks (e.g. 3G, DSL) and for roaming through links to other CSNs.

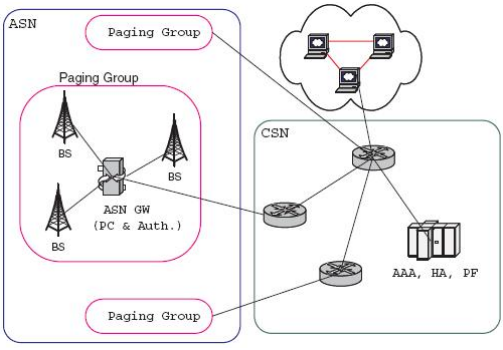

Fig. 1. WiMAX Reference Network Model

3.2 Bandwidth Allocation for Ranging

When a subscriber station (SS) attempts initial entry to the network, first it requests bandwidth by using RNG-REQ and Ranging Response (RNG-RSP) messages [12]. Figure 2 shows the initial entry process.

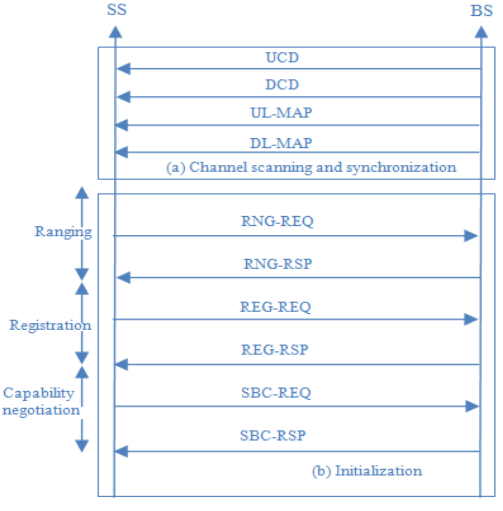

Fig. 2. Initial entry process

In its down link (DL) channel, the BS decides on allocating bandwidth to SSs per CID (Connection Identifier, connections are identified by a connection identifier. A 16-bit value that identifies a connection or an uplink/ downlink pair of associated management connections to equivalent peers in the medium access control layer of the BS and SS. The CID address space is common between DL and UL and partitioned among the different types of connections) basis and does not requires the SSs to be involved. The BS always reserve required bandwidth for ranging interval

which is indicated in Uplink-MAP (UL-MAP). To get bandwidth for ranging, an SS chooses an appropriate ranging code to transmit during the ranging interval. On successful reception of the code, the BS assigns proper bandwidth to the SS for ranging [13]. As Figure 2 shows, there is no authentication or authorization for granting bandwidth any SS can request bandwidth for ranging. This procedure provides a possibility of DDoS attack to BS and ASN-GW for malicious SSs to generate as many fraudulent requests as they intend to [4].

3.3 Attacks to BS and ASN GW

To connect to a network, an SS attempts to determine whether it is in the coverage of a suitable WiMAX network first. The SS stores a permanent list of all operational parameters of the connecting network, such as the DL (Downlink, the direction from the base station to the subscriber station) frequency used during the previous connection operation [12]. The MS first attempts to synchronize with the stored DL frequency if this fails, then scans other frequencies in an attempt to synchronize with the DL of the most suitable BS. During the DL synchronization, the MS listens for the DL frame preambles. When one is detected the MS can synchronize itself to the DL transmission of the BS. Once it obtains DL synchronization, the MS listens to the various control messages, such as DCD, UCD, DL-MAP, and UL-MAP, that follow the preamble to obtain the PHY- and MAC related parameters corresponding to the DL and UL (Uplink, the direction from a subscriber station to the base station) transmissions [13]. The initial entry process has 6 stages. Stage 1 and 2 that include synchronization and initial ranging are shown in figure 2. A RNG-REQ is transmitted by the SS at initialization periodically to determine network delay and to request power and/or DL burst profile change [12]. This message has a standard syntax that specifies type, size and the value of the request. An attacker may misuse RNG-REQ message, changing some fields randomly and send it to BS in large volume to waste the resources of the network.

4 Detection System

The goal of the proposed system is to provide an environment to analyze the network traffic under the DDoS attack more efficiently. In this section first statistical preliminaries will be introduced, and then an efficient traffic modeling for extracting features will be presented.

4.1 Statistical Preliminaries

To perform the DDoS attack, the attacker usually sends large amount of RNG-REQ messages to the BS changing the address field of the messages randomly. So we can exploit entropy concept to measure the dispersion of the addresses sent to the BS, because in the attack state the dispersion of the addresses is higher than the normal state.

The entropy of a random variable X measures the uncertainty of X , and is defined as:

$$E(X) = -\sum_{i=1}^{n} P(X = x_i) \log_2 P(X = x_i) \quad (1)$$

Where $x_1, x_{2,\ldots,} x_n$ are the values within the given range for X and $P(x_i)$ shows the probability that X takes the value x_i and is defined as:

$$P(X = x_i) = \frac{m_i}{m} \quad (2)$$

Where m_i is the number of the messages with x_i as the destination address and m represents the number of the total addresses within the epoch.
The normalized entropy is defined as:

$$E_n(X) = \frac{E(x)}{\log N_0} \quad (3)$$

Where N_0 represents the number of different addresses within the specified epoch and $\log N_0$ is the normalization factor.

In mobile WiMAX networks whenever an SS try to join the network, it should send a RNG-REQ message to BS; moreover, there are other situations in which the SSs send RNG-REQ messages toward the BS. So in detecting the attack we can consider just RNG-REQ messages sent in the initial network entry. The situations in which an SS also sends RNG-REQ messages to BS are as follow:

- Re-entry to network from idle mode: If an MS has some pending traffic or its security context is going to expire, it should perform re-entry to network from idle mode. Also after De-Registering from the network, the SS enters idle mode. Idle mode re-entry to network is the same as the initial network entry except that some procedures are omitted. In order to perform re-entry to network from idle mode, the MS should send RNG-REQ message to the BS, but in this case some parameters of the messages are different.
- Keep-alive check in sleep mode: In order for a BS to maintain supervision of MSs in sleep mode and to perform necessary adjustments, BS may implement a keep-alive check mechanism which includes sending RNG-REQ message to BS.
- Handover: When a mobile station tries to switch between two BSs and migrates from the air-interface provided by one base station to the air-interface provided by another BS, it should perform handover process. In order to perform handover it should send a RNG-REQ message to BS.
- Location update: There are two location update procedures, secure location update and unsecure location update. In secure location update, MS first sends a RNG-REQ message including the CMAC tuple to the BS.

In all the above situations since the MS has once joined the network, a CID has been assigned to it which is different from the CID assigned to the MS during the initial

network entry process. So RNG-REQ messages sent to BS in other situations except the initial network entry can be seprated using the conditional entropy. So we can use Conditional Entropy to get more information from the received messages. The conditional entropy quantifies the remaining entropy or uncertainty of a random variable Y given that the value of another random variable X is known.

The Conditional Entropy measures the uncertainty of the variable X considering the variable Y and is defined as:

$$H(X|Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m}(P(X = x_i, Y = y_j).\log P(X = x_i \mid Y = y_j)) \quad (4)$$

Where $P(X|Y)$ represent the probability of X considering Y, and is defined as:

$$P(X|Y) = \frac{P(X \cap Y)}{P(Y)} \qquad P(Y) > 0 \quad (5)$$

Considering X as the RNG-REQ messages with x_i as the MAC address sent to BS and Y as the RNG-REQ messages sent to BS as none of the following purpose,

- Re-entry to network from idle mode
- Keep-alive check in sleep mode
- Handover
- Location update

We calculate the conditional entropy of the message to extract more efficient information from network traffic to detect the attack.

Another statistical concept which helps us in detecting the attack is called Mutual Information. The mutual information parameter I (X;Y) is defined as:

$$I(X;Y) = H(X) - H(X|Y) \quad (6)$$

Note that before considering Y, the uncertainty of X is H(x), after observing and considering it, this uncertainty goes down to H(x|y). Therefore, the mutual information measures the amount of information we learn about X by considering Y. In our analysis, we would like to estimate the value of X based on the observation of Y, which includes the real attack messages and the normal legitimate accessing messages. Recall that the conditional entropy measures how much uncertainty remains for X given considering Y.

4.2 Modeling the Network Traffic

The arrival process of packets to the network has been mostly modeled by Poisson process; however, recently it is shown that the self-similar model is more appropriate for heavy loaded network traffic [14]. The traffic of internet based protocols show that traffic variation exists in large time slots and the traffic in smaller slots is correlated to the traffic in larger slots. In fact, the traffic of heavy loaded networks can

be modeled by fractal time series which have the self-similarity and Long Range Dependency (LRD) properties [15]. Based on the LRD properties of the traffic, in the phase of extracting network traffic features, at the end of specified given epochs a vector is extracted. The more epochs are smaller, we have less delay, but we cannot choose the epochs smaller than a specified threshold, because in this case we may lose some useful data. The dataset is split in to non-overlapping epochs consisting of flows that completed within.

5 Experimental Results and Discussion

Most of the works done so far, assume that low volume of traffic has been used for DDoS attack, and the target network is not centralized. In contrast, the recent Mobile WiMAX networks are centralized and expected to handle considerable volume of data traffic, so that DDoS attack needs to be revisited. In our research, to analyze the attack traffic, first the Reference Network Model (RNM) is simulated by OPNet where some of the SSs generate the attack traffic. Our data set uses flow data captured in the OPNet simulation environment consisting of the traffic from normal and malicious SSs sent to the BS. In the following the entropy resulted from network traffic is presented.

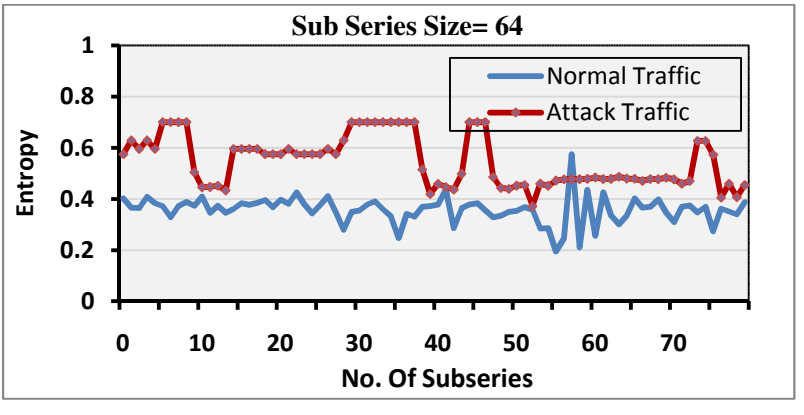

Fig. 3. The Entropy of the address of received messages, subseries=64

Table 1. Max, min and average value of the Entropy in figure 3

Entropy	Average	Min Value	Max Value
Normal Traffic	0.35797674	0.194652912	0.574149885
Attack Traffic	0.561667515	0.371713305	0.7

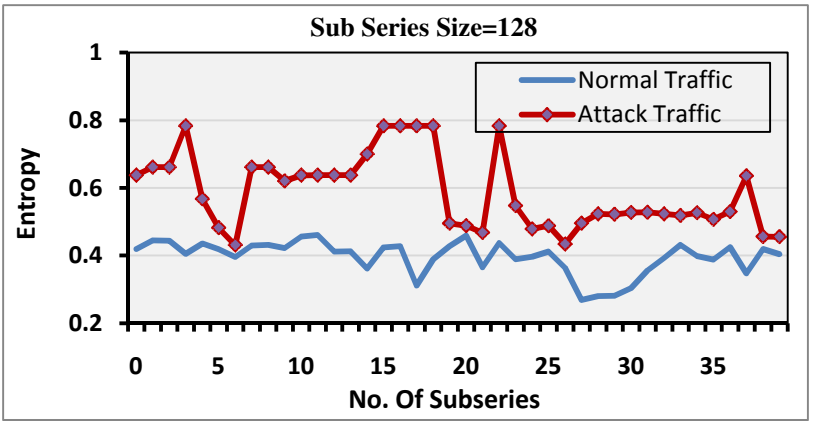

Fig. 4. The Entropy of the address of received messages, subseries=128

Table 2. Max, min and average value of the Entropy in figure4

Entropy	Average	Min Value	Max Value
Normal Traffic	0.403591572	0.311654769	0.460956424
Attack Traffic	0.626945912	0.43119818	0.783333333

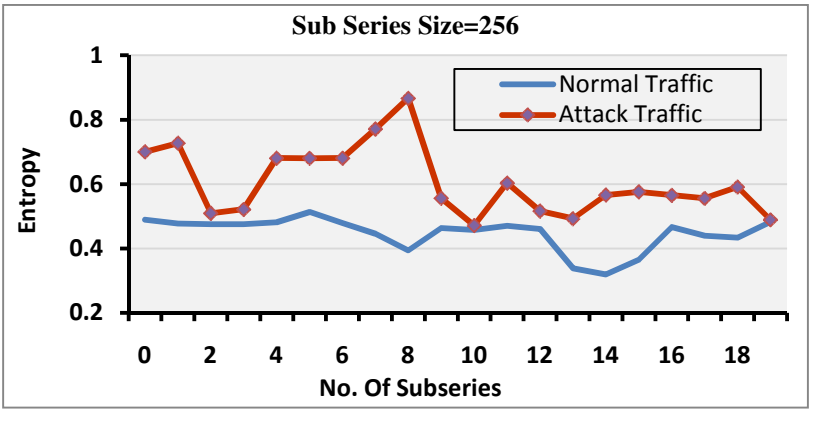

Fig. 5. The Entropy of the address of received messages, subseries=256

Table 3. Max, min and average value of the Entropy in figure5

Entropy	Average	Min Value	Max Value
Normal Traffic	0.480466913	0.475319062	0.512722339
Attack Traffic	0.636584255	0.509325773	0.727359224

Assuming the size of subseries to be 64, 128 and 256 respectively, the figures 5, 6 and 7 show the entropy value of the MAC address of the received messages in normal and attack state. The tables 1, 2 and 3 show the minimum, maximum and average value of the estimated entropy in these three cases. According to the irregular dispersion of the addresses in the attack state, the estimated entropy in the attack state is more than the estimated entropy of the normal state. On the other hand, estimating the entropy based on different subseries size show that the entropy value of the network traffic with subseries size of 128 varies between 0.3116 and 0.4609 in normal state and in the attack state it varies between 0.4311 and 0.7833. By making the subseries bigger and assuming the subseries size to be 256, it is seen that the entropy varies between 0.4753 and 0.5127 in the normal state and between 0.5093 and 0.7273 in the attack state. By choosing smaller subseries size, it is seen that the results are to some extent closer to results achieved by subseries size of 128. Comparing the results in three different condition shows that big subseries have less precision and give us less information about the network traffic in comparison with subseries of smaller size. Also it is shown that analyzing the network traffic with subseries size of 64 has more precision than the other two conditions, because there is a bigger difference between the entropy in the normal and attack state which help us to detect the attack more precisely. The more the difference between the entropy of the attack state and normal state is higher, the more precise the detection of the attack is. After calculating the entropy of the received messages, to get more information from the network traffic the conditional entropy of the network traffic is estimated. Then based on the entropy and conditional entropy, more precise information can be extracted from the network traffic to help us in detecting the attack which is called Mutual Information. In the following first the results achieved by calculating the conditional entropy will be presented then the mutual information of the entropy and conditional entropy will be presented.

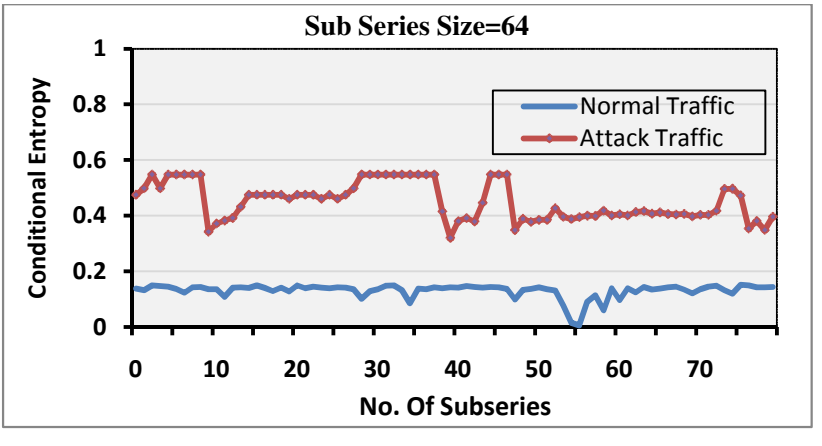

Fig. 6. The Conditional Entropy of the address of received messages, subseries=64

Table 4. Max, min and average value of the Conditional Entropy in figure6

Conditional Entropy	Average	Min Value	Max Value
Normal Traffic	0.12878809	0.00565246	0.150011
Attack Traffic	0.460910558	0.32036791	0.547494

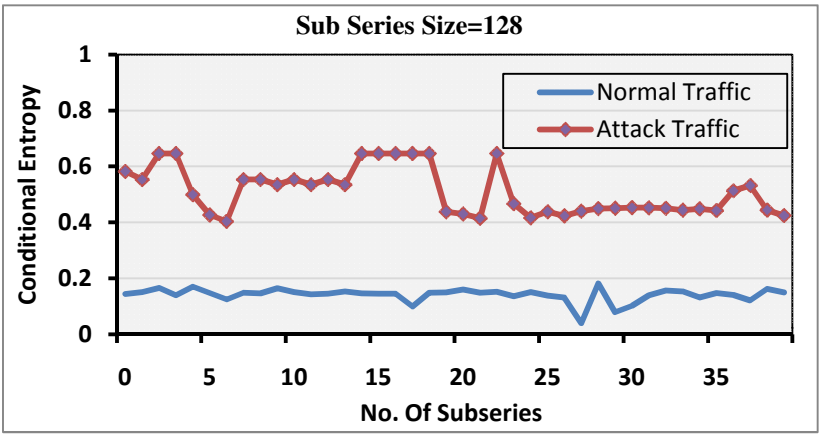

Fig. 7. The Conditional Entropy of the address of received messages, subseries=128

Table 5. Max, min and average value of the Conditional Entropy in figure7

Conditional Entropy	Average	Min Value	Max Value
Normal Traffic	0.14735965	0.099296019	0.170450176
Attack Traffic	0.54489437	0.40383335	0.646462667

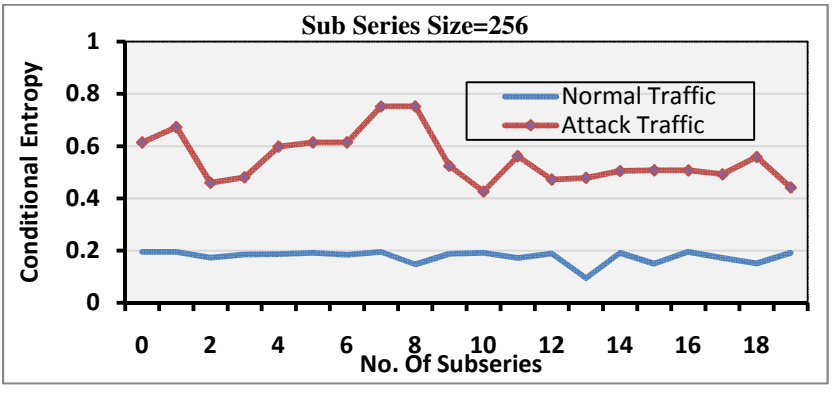

Fig. 8. The Conditional Entropy of the address of received messages, subseries=256

Table 6. Max, min and average value of the Conditional Entropy in figure8

Conditional Entropy	Average	Min Value	Max Value
Normal Traffic	0.186677367	0.172669932	0.195040818
Attack Traffic	0.579264891	0.459405771	0.673525469

Assuming the size of subseries to be 64, 128 and 256 respectively, the figures 8, 9 and 10 show the conditional entropy value of the MAC address of the received RNG-REQ messages considering the four states mentioned in the previous section, in normal and attack state. The tables 4, 5 and 6 show the minimum, maximum and average value of the estimated conditional entropy in these three cases. According to the irregular dispersion of the addresses in the attack state and the estimated conditional entropy, it is seen that the estimated conditional entropy in the attack state is more than the estimated value in the normal condition, but on the other hand by comparing it with the estimated entropy it is seen that it has gone down to some extent, because in this case some of the messages are ignored and are not considered. Moreover, comparing the resulted graphs with three different subseries show that with subseries size of 256 the conditional entropy varies between 0.172 and 0.1950 in the normal state and between 0.4594 and 0.6735 in the attack state, but by assuming the subseries size smaller, it is seen that in the case of subseries size of 64 it varies between 0.0056 and 0.15 in the normal state and between 0.3203 and 0.5474 in the attack state. So it can be concluded that smaller subseries size are more precise than bigger ones and give us more information about the network traffic.

Following graphs present the Mutual Information parameter information of the network traffic, achieved by the estimated Entropy and Conditional entropy of the network traffic.

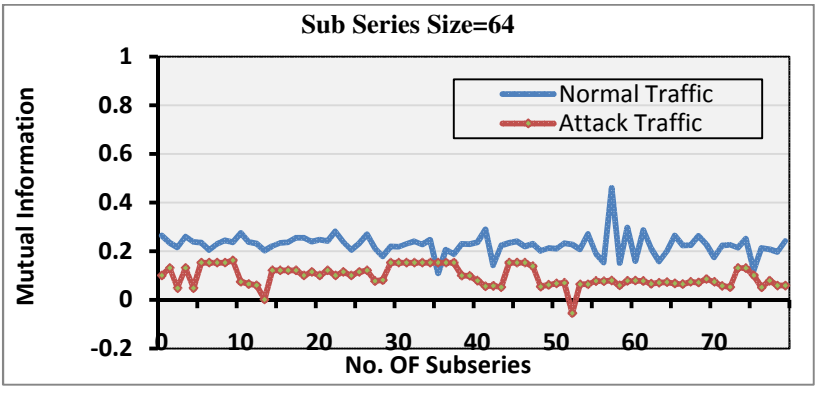

Fig. 9. The Mutual Information of the Entropy and Conditional entropy of received messages, subseries=64

Table 7. Max, min and average value of the Mutual Information parameter in figure9

Mutual Information	Average	Min Value	Max Value
Normal Traffic	0.229157	0.109292	0.46005
Attack Traffic	0.096786	-0.05491	0.161787

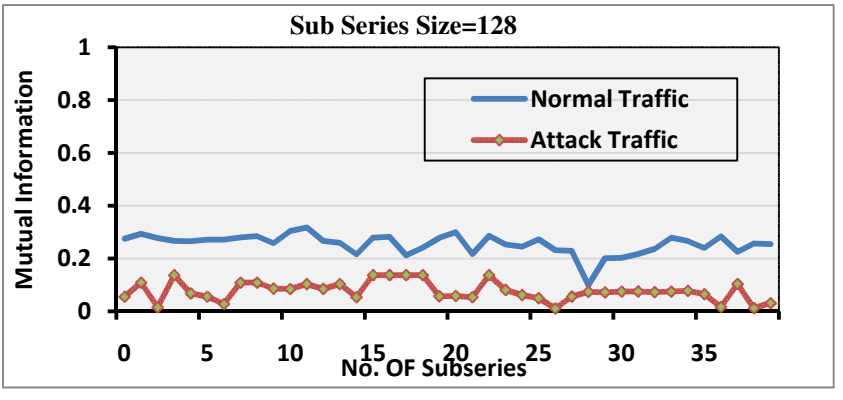

Fig. 10. The Mutual Information of the Entropy and Conditional entropy of received messages, subseries=128

Table 8. Max, min and average value of the Mutual Information parameter in figure10

Mutual Information	Average	Min Value	Max Value
Normal Traffic	0.255822	0.098504321	0.317333
Attack Traffic	0.081454	0.010591804	0.136871

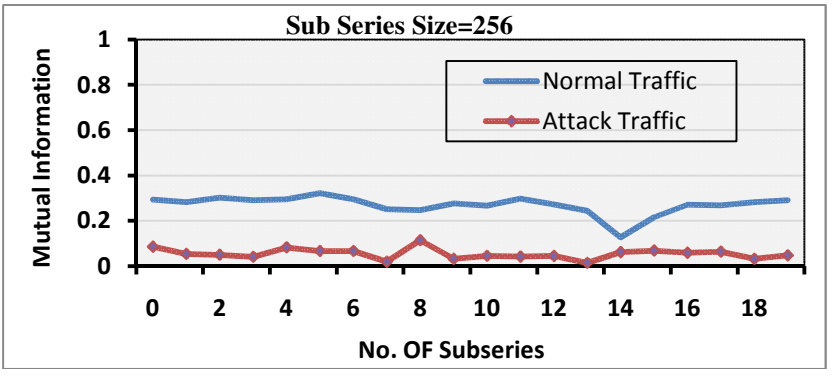

Fig. 11. The Mutual Information of the Entropy and Conditional entropy of received messages, subseries=256

Table 9. Max, min and average value of the Mutual Information parameter in figure11

Mutual Information	Average	Min Value	Max Value
Normal Traffic	0.297452	0.282255	0.32227
Attack Traffic	0.063164	0.040992	0.085665

Assuming the size of subseries to be 64, 128 and 256 respectively, the figures 11, 12 and 13 show the Mutual Information parameter value of the MAC address of the received RNG-REQ messages considering Entropy and Conditional Entropy value of the received traffic. The tables 7, 8, and 9 present the maximum, minimum and average value of the estimated Mutual Information parameter. The resulted Mutual Information parameter shows that the value of this parameter in normal state is higher than its value in attack state. Because in the normal state some of the RNG-REQ messages sent to BS may be sent as one of the four purposes mentioned in the previous section, so there is a difference between the resulted Entropy and Conditional Entropy, while in the attack state the ratio of these kinds of messages is low and there is no so much difference between the estimated Entropy and Conditional Entropy. According to the resulted graphs, in the attack state, the Mutual Information parameter varies between 0.2822 and 0.3222 when the size of subseries is considered to be 256 in the normal state and between0.0409 and 0.0856 in the attack state. By changing the subseries size to a smaller size, 64, the Mutual information parameter varies between 0.1092 and 0.96 in the normal state and between -0.0549 and 0.1617 in the attack state. So considering the estimated results and this fact that, the more the difference between Entropy and conditional Entropy is less the more information can be extracted from the network traffic, we conclude that totally the precision of the resulted parameters in the case of subseries size of256 is more than the other two cases.

6 Conclusion and Future Works

In this paper we presented an analytical model for WiMAX network traffic under DDoS attack and evaluated the Entropy, Conditional Entropy and Mutual Information parameters of the traffic in both normal and attack states. According to the simulation results, as the statistical properties of the attack traffic pattern differ from the ones for the normal traffic pattern, the attack can be detected using extracted statistical properties of the traffic. The difference between our proposed system and the existing system is that we had a different look at the arrival process of the messages to the BS. Since recently it is shown that the self-similar model is more appropriate for heavy loaded network traffic, we exploited this property and evaluated the network traffic with three different subseries size. For the future work, the results of this paper can be used to train an artificial neural network to detect DDoS attacks. Artificial Neural Networks in order to distinguish between the attack state and normal state need some feature to feed the network, so the results of this research will be used to train the network and identify the attack.

Acknowledgement. This work is supported by Iran Telecommunication Research Center (ITRC).

References

[1] Vafea, A.: Security of IEEE 802.16. Master of Information and Communication Systems Security, Department of Computer and Systems – Science Royal Institute of Technology (2006)
[2] Jamshed, H.: Security Issues of IEEE 802.16 (WiMAX), School of Computer and Information Science, Edith Cowan University, Australia (2006)
[3] Eren, E.: WiMAX Security Architecture – Analysis and Assessment. In: IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications Dortmund, Germany, September 6-8 (2007)
[4] Youngwook, K., Hyoung-Kyu, L., Saewoong, B.: Shared Authentication Information for Preventing DDoS attacks in Mobile WiMAX Networks. In: IT R&D program of MIC/IITA. IEEE, Korea (2007)
[5] Shon, T., Choi, W.: An Analysis of Mobile WiMAX Security: Vulnerabilities and Solutions. In: Enokido, T., Barolli, L., Takizawa, M. (eds.) NBiS 2007. LNCS, vol. 4658, pp. 88–97. Springer, Heidelberg (2007)
[6] Boom, D.: Denial of Service Vulnerabilities in IEEE 802.16 Wireless Networks. Master Thesis at Naval Postgraduate School Monterey. IEEE, California (2004)
[7] Nasreldin, M., Aslan, H., El-Hennawy, M., El-Hennawy, A.: WiMAX Security. In: 22nd International Conference on Advanced Information Networking and Applications, IEEE (2008)
[8] Lee, K., Kim, J., Kwon, K.H., Han, Y., Kim, S.: DDoS attack detection method using cluster analysis. ESWA 34, 1659–1665 (2008)
[9] George Nychis, V.S., Andersen, D.G., Kim, H., Zhang, H.: An Empirical Evaluation of Entropy-based Traffic Anomaly Detection. In: IMC 2008. ACM, Greece (2008)
[10] Zhou, W., Yu, S.: Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks. In: Sixth Annual IEEE International Conference on Pervasive Computing a and Communication (2008)
[11] Kar, S., Sahoo, B.: An Anomaly Detection System for DDoS Attack in Grid Computing. International Journal of Computer Applications in Engineering, Technology and Sciences (ij-ca-ets) 1, 553 (2009)
[12] IEEE Standard 802.16-2009: Air Interface for Broadband Wireless Access Systems (May 2009)
[13] Taylor & Francis Group, WiMAX/MobileFi, Auerbach (2008) ISBN 978-1-4200-4351-8
[14] Karagiannis, T., Molle, M., Faloutsos, M.: Long Range Dependence. IEEE Computer Society (2004) 1089-7801/04/$20.00
[15] Millán, G., Lefranc, G.: Presentation of an Estimator for the Hurst parameter for a Self-similar Process Representing the Traffic in IEEE 802.3 Networks. Int. J. of Computers, Communications & Control IV(2), 137–147 (2009) ISSN 1841-9836, E-ISSN 1841-9844