BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **14**, No 1

Sofia • 2014 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2014-0002

RQA Based Approach to Detect and Prevent DDoS Attacks in VoIP Networks

N. Jeyanthi, R. Thandeeswaran, J. Vinithra

School of Information Technology and Engineering,
VIT University, Vellore -632014, Tamilnadu, India
Email: njeyanthi@vit.ac.in

Abstract: *Voice over Internet Protocol (VoIP) is a family of technologies for the transmission of voice over Internet. Voice is converted into digital signals and transmitted as data packets. The Session Initiation Protocol (SIP) is an IETF protocol for VoIP and other multimedia. SIP is an application layer protocol for creating, modifying and terminating sessions in VoIP communications. Since SIP is a more flexible and simple protocol, it is quite easy to add features to it.*

Distributed Denial of Service Attack (DDoS) floods the server with numerous requests from various hosts. Hence, the legitimate clients will not be able to get their intended services. A major concern in VoIP and almost in all network domains is availability rather than data consistency. Most of the surviving techniques could prevent VoIP network only after collision. This paper proposes a Recurrence Quantification based approach to detect and prevent VoIP from a DDoS attack. This model detects the attack at an earlier stage and also helps to prevent from further attacks. In addition, this techniques enables the efficient utilization of resources. QUALNET has been used to simulate the operation of the proposed technology.

Keywords: *VoIP, SIP, Distributed denial-of-service attacks, Recurrence Quantification Analysis***.**

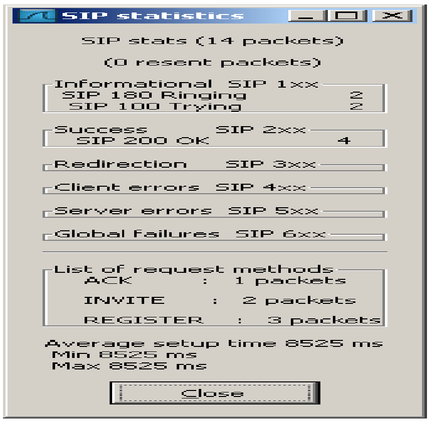
1. Introduction

Voice over Internet Protocol (VoIP) [1] is a technology which enables transmission of voice over Internet. The sound signals are digitalized compressed and sent as packets over Internet. The major advantage of VoIP is that it does not charge any extra tolls like the traditional communication systems do. It thus enables fast and cost efficient data transfer over Internet Protocol. There is a claim that VoIP will soon replace all the existing telecommunication media.

The Session Initiation Protocol (SIP), an alternative to H.323, is a part of the Internet Engineering Task Force standard process for transmission [2] of real time audio, video, and data over Internet. It is modelled on other Internet protocols, such as HTTP and SMTP. SIP, an application layer signalling protocol (end-to-end), is used to set up, modify and terminate multimedia sessions in Internet. SIP INVITE messages are used to create sessions. They carry the session descriptions that allow participants to agree on a set of compatible media types. SIP makes use of elements, called proxy servers, to help route requests to the user's current location, authenticate and authorize users for services, implement provider call-routing policies, and provide other features to users.

SIP also provides a registration function [3] that allows users to upload their current locations for use by proxy servers. REGISTRAR is the server responsible for this task and the information about the user agents is stored in location servers. Once the session is established, the actual data is carried over RTP packets. In DDoS attacks [4], an attacker will compromise many systems distributed across the network and command them to start sending requests to the target. This leads to exhaustion of the target's resources, such as memory, bandwidth, CPU, etc. Due to the enormous requests from the attackers, the victim fails to process and serve the legitimate users.

In VoIP networks [5], the flooding attack is the most severe threat. The SIP proxies are flooded up by thousands of INVITE requests simultaneously or within a short period of time. The servers have to maintain the state of each INVITE message while it is waiting for the OK message. These states can be calling, trying, ringing, etc. In case of severe attacks, the resources of the proxies being attacked are exhausted. A registration process also makes bed for a DDoS attack, as there is no authentication of the REGISTER messages. The attackers can make numerous REGISTER requests and thereby flood the Register and Location Servers, as shown in Fig. 1. Fig. 1 shows the statistics of the scenario given in Fig. 2. The average time for a call setup is 8525 ms. There are 2 INVITE packets, 3 REGISTER packets (sender, proxy and receiver) and 1 ACK packet (the 2nd session is not completed).

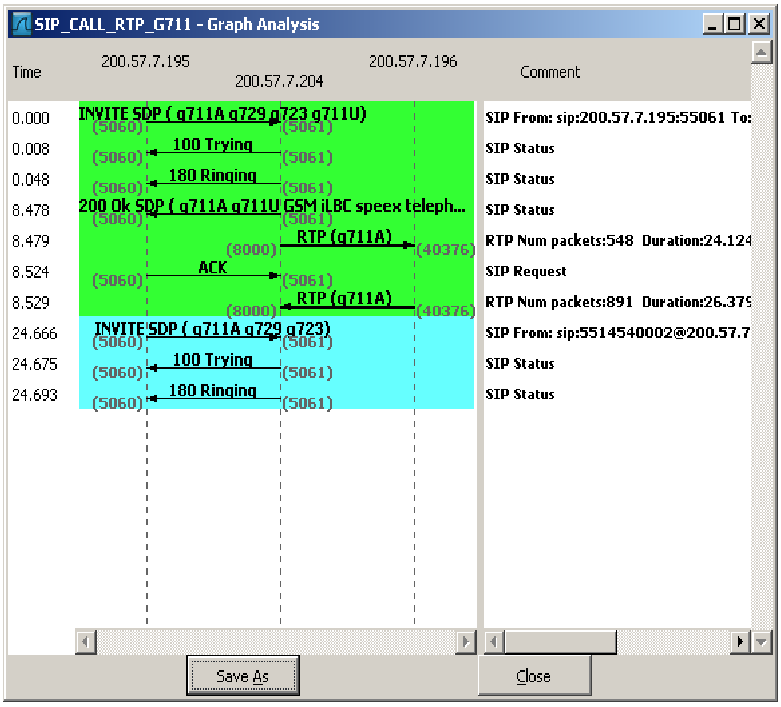


```
SIP stats (14 packets)
(0 resent packets)

Informational  SIP 1xx
 SIP 180 Ringing          2
  SIP 100 Trying          2

Success        SIP 2xx
   SIP 200 OK            4

Redirection     SIP 3xx
Client errors  SIP 4xx
Server errors  SIP 5xx
Global failures  SIP 6xx

List of request methods
    ACK         :   1 packets
    INVITE      :   2 packets
    REGISTER    :   3 packets

Average setup time 8525 ms
 Min 8525 ms
 Max 8525 ms
```

Fig. 1. SIP session initiation statistics

In Distributed Reflection DoS, the attacker generates a large number of fake requests with spoofed IP addresses in the SIP message header. This fools the server by identifying the target host as the sender of requests. This can lead to flood of the server, as well as the target host. The server will be flooded by the fake requests and the target host will be flooded by the responses from the server. The proposed work focuses on SIP based Denial of service attacks.

The session is initiated and established using various SIP messages: in Fig. 2 the user agent, having IP address 200.57.7.195 sends an INVITE message to the user agent having IP address 200.57.7.196 through the proxy server 200.57.7.204.



Time	200.57.7.195	200.57.7.204	200.57.7.196	Comment
0.000	(5060) INVITE SDP (g711A g729 g723 g711U)	(5061)		SIP From: sip:200.57.7.195:55061 To:
0.008	(5060) 100 Trying	(5061)		SIP Status
0.048	(5060) 180 Ringing	(5061)		SIP Status
8.478	(5060) 200 Ok SDP (g711A g711U GSM iLBC speex teleph...	(5061)		SIP Status
8.479		(8000) RTP (g711A)	(40376)	RTP Num packets:548 Duration:24.124
8.524	(5060) ACK	(5061)		SIP Request
8.529		(8000) RTP (g711A)	(40376)	RTP Num packets:891 Duration:26.379
24.666	(5060) INVITE SDP (g711A g729 g723)	(5061)		SIP From: sip:5514540002@200.57.7
24.675	(5060) 100 Trying	(5061)		SIP Status
24.693	(5060) 180 Ringing	(5061)		SIP Status

Fig. 2. SIP connection control

The proxy will send back the sender 100 trying messages and then 180 ringing messages, which is an indicator that the call is ringing at the destination. The callee accepts the call and sends 200 OK messages. The caller acknowledges the 200 OK messages by sending an ACK. The session is established now. All further transactions take place without the intervention of proxies as RTP packets.

This paper proposes a Mathematical approach, called Recurrence Quantification Analysis for detection and hence, prevention of a DDoS attack. It monitors the traffic continuously at each point and detects any deviation from the normal traffic behaviour. Moreover, unlike many other schemes that are based on one or two parameters for detecting the attack, RQA makes use of various measures, like Recurrence Rate, Determinism, Entropy, Laminarity, etc., which contribute to the efficiency if the method.

The rest of the paper is organized as follows: In Section 2, a review of related works is done. Section 3 defines the proposed approach. Section 4 is about the experimental set up. Section 5 concludes the paper, followed by References section.

2. References survey

Mathematical models could analyze the traffic behaviour and performance issues in a better perspective. Few of them were studied and their analysis presented over here.

Covariance Analysis model [6] is a statistical model for detection of DDoS attacks. There is not any presumption on the network traffic distribution. The pattern of the normal traffic differs from the attack traffic in terms of correlation. This correlation is taken as a parameter for indication of the change. It uses all the flags in the TCP header field. In SYN flooding attack, the values in the SYN and FIN fields mismatch. The covariance of each pairs of flags in the header is used to detect the SYN flooding attack. This method is not so reliable because the flags which are used as a parameter for detecting the attack can be altered. Besides, the time interval for packet selection is not following any particular method.

Entropy-based Input-Output traffic mode [7] compares the entropy of normal traffic and attacked traffic. The entropy of traffic tends to drop down when an attack occurs. The problem here is that the attackers can modify the attacking method if they came to know about the detection strategy. In DDoS Attacks Detection Using GA based Optimized Traffic Matrix [8], a traffic matrix is created with a packet based window and a simple hash function is used to map the analyzed traffic to this matrix. The parameters used are optimized, using a Genetic Algorithm. However, the usage of a hashing function which may lead to collision has to be dealt with.

The Agent-based Instruction Detection System uses Chi-Square statistical method [9] for DDoS attack detection. Mobile agents distributed over the network decentralize the task of traffic collection, analysis of data and reduce the workload. Router Based Detection for Low-Rate Agents of DDoS Attack [10] is proposed for low rate flooding detection. It is based on the TCP SYN-SYN/ ACK pairs in the header field of TCP. The incoming packets are classified into two streams. The ACK number and ISN are compared. The difference between the number of SYN packets and the number of packets is normalized. CPO uses this normalized difference to decide whether the attack has occurred or not. All Point-of-Presence in ISP domain is associated with the detection process [11]. The communication overhead here between the points and the coordinator router for analysis is a demerit of this method.

A Coordinated Detection and Response Scheme [12] makes use of two types of agents namely, Stub Agent (SA) and Transit Agent (TA). Attack traffic and genuine traffic pass through the Source side SA (SSA), TA and finally through the Victim side SA (VSA), before reaching the victim. The SA monitors the traffic and if any abnormality is detected, it informs the nearest TA. CUSUM is used to detect abnormalities. TA broadcasts about the attack to all SAs. A marker field is usually set to determine the valid addresses. But in cases of spoofed attacks, a counter is used to know the number of packets sent within a tine window.

In Fine-Grained DDoS Detection Scheme [13], a Bidirectional Count Sketch is proposed. Asymmetry of the attack traffic is used to detect an attack. The server exhibits a larger value of the asymmetry index if it is under an attack. The statistics of SYN arrival rate is investigated [14] and compared with two levels of the threshold. If the analyzed traffic's SYN arrival rate exceeds the threshold, an attack is detected. A second threshold, incomplete three-way handshaking SYN packet Ratio, is also set up that detects low rate DDoS attacks. The detection mechanism has low false positive and false negative rate, and high detection accuracy. DDoS attack detection based on wavelet analysis [15] is used with discrete wavelet transform technique to detect the DDoS attack. Rapid detection of the attack is possible using this method. But this method depends on the traffic statistics before the detection and it is also influenced by the wavelet basis functions.

Flexible Deterministic Packet Marking [16] allows adjusting of the length and rate of marking based on the protocol being used and on the load upon the router. But the packet processing consumes more memory space and computing capacity of the participating routers and in case of high traffic, the router will be overloaded, which is a question of performance.

In [18] an integrated approach is quoted. The defence requirement for each phase of the attack is explored in this scheme. In this approach all information regarding the security and network related components, are collected first. The collected information are then integrated and analyzed. An Integrated DDoS Attack Defence Infrastructure is located at the centre of the networks, so that information gathering will be more efficient. Real-time DDoS attack responses and tracing back is possible.

In Middleware-based Approach for Preventing DDoS Attacks [19], large scale attacks are defended. It makes use of a Virtual private Operation Environment to prevent the attack. Middleware boxes are installed at various points in the network. This helps the others to reduce resource allocation and all. The middleware boxes in one domain cooperate with other domains' middleware boxes in order to improve the methods efficiency.

In provider-based deterministic packet marking against DDoS attacks [20], the victims are protected by limiting the amount of large traffic during the attack and leaving the legitimate traffic unaffected. The marking scheme aims at providing the victim's provider with secure and reliable information about the incoming traffic path. History-based IP filtering edge routers permit the incoming packets based on the entries in a pre-built database which is built on the history of packets received by that router earlier. Route-based distributed packet filtering [21] filters the spoofed IP packets and prevents them from reaching the destination. The route is used as a parameter for filtering. This is not so reliable because the route may change in real time. Scalability is also an issue, and the global knowledge of the network infrastructure.

The proposed RQA approach might detect the attack at an early stage and also vary dynamically based on the traffic fluctuation.

3. Recurrence Quantification Analysis

3.1. Recurrence phenomenon

Recurrence Quantification Analysis is a technique to analyze the behaviour of non-linear traffic data. The recurrence property [17] of a dynamic system allows it to migrate to a new state in case of any disturbance and to restore either to the original state or closer to it. A Recurrence Plot (RP) is a visualization [29, 30] of the dynamic states with a square matrix showing state x at time i and j. It consists of dots and lines. The dots may be black or white, the black dot indicating the recurrence. The lines may be horizontal, vertical or parallel to the mean diagonal (LOI, Line of Identity). The diagonal lines indicate that the evolution of the state is similar at different times. The vertical and horizontal lines indicate that the states are not changing with time. RQA quantifies this RPs. A recurrence plot can be mathematically represented as:

(1) $$R(i,j) = u\left(\varepsilon - \left(\left\|x_i - x_j\right\|\right)\right), \; i, \; j = 1 \ldots N,$$

where N is the number of states under consideration, ε is the threshold distance and $\|.\|$ is a norm and u is the Heaviside function.

The norm can be a maximum norm, minimum norm and Euclidean norm. The recurrence area is largest for the maximum norm, smallest for the minimum norm, and intermediate – for the Euclidean norm. Heaviside step function, also called a unit step function, has a value of zero for negative arguments and one for positive arguments.

(2) $$u(x) = \begin{cases} 0, & x < 0, \\ 1, & x \geq 0. \end{cases}$$

3.2. Recurrence parameters

Recurrence Rate is the probability of a particular state to recur. The percentage of the recurrence quantifies the percentage of recurrent points falling within the specified radius, ranges from 0 up to 100%.

(3) $$\text{RR} = [\text{sum of all } R(i,j)]/N_2.$$

Determinism is the ratio of recurrence points, forming diagonal structures to all points in the RP which vary according to the types of the signal. Periodic signals make very long diagonal lines; very short diagonal lines represent chaotic signals, whereas stochastic signals have no diagonal lines at all.

(4) $$\text{DET} = [\text{sum of all } l \times P(l)]/RR,$$

where $P(l)$ is the frequency of diagonal lines with length l=$l$min to N.

Laminarity is the ratio of recurrence points forming vertical structures to all points in the RP

(5) $$\text{LAM} = [\text{sum of all } v \times P(v)]/RR$$

where $P(v)$ is the frequency of vertical lines with length $v = v_{\min}$ to N.

Trapping time, the average length of vertical lines, determines how long a system remains in a specific state

(6) $$\mathrm{TT} = \mathrm{LAM}/\text{Total no. of vertical lines}.$$

Divergence, the reciprocal maximal diagonal line length (without LOI), estimates the positive maximal Lyapunov exponent of the dynamical system.

(7) $$\mathrm{DIV} = 1/L_{\max}.$$

Entropy is Shannon's entropy of the probability $p(l)$ that a diagonal line has length exactly equal to l,

$$p(l) = P(l)/[\text{sum of all } P(l)] \text{ where } l = l_{\min} \text{ to } N,$$

(8) $$\mathrm{ENTR} = -\text{sum of all } [p(l) \times \ln p(l)]. \qquad \ldots$$

Trend is the measure of the tendency that the recurrence points will move away from the mean diagonal. This quantifies the degree of system stationarity. Homogenous distribution of the points in the recurrence plot shows the trend value to be around zero and heterogeneous distribution shows it deviating from zero. The recurrences parameters are analyzed and based on the deviation of these parameters from the normal value, they are considered as an attack, thereby DDoS attack is detected, as shown in Fig. 4.

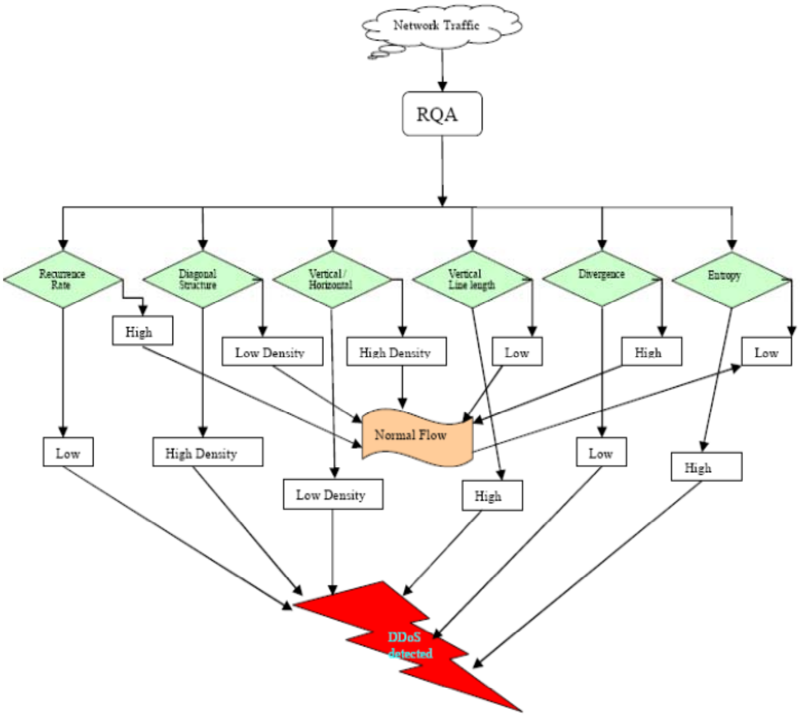


Fig. 4. DDoS detection with the aid of RQA parameters

4. Experimental setup

Two scenarios of a VoIP network, with and without a DDoS attack, are simulated using Qualnet. A sample architecture of the simulated scenarios is as follows:

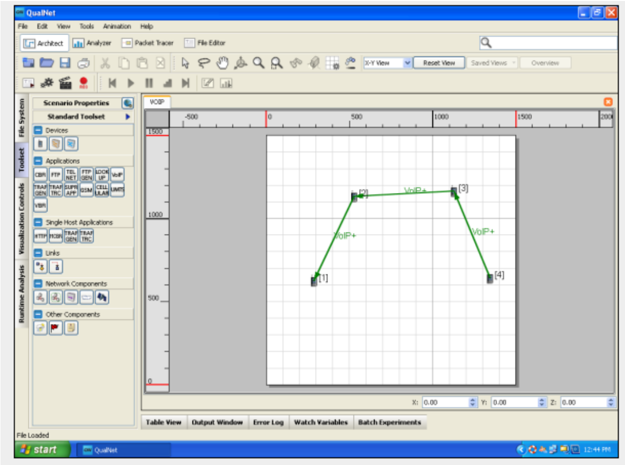
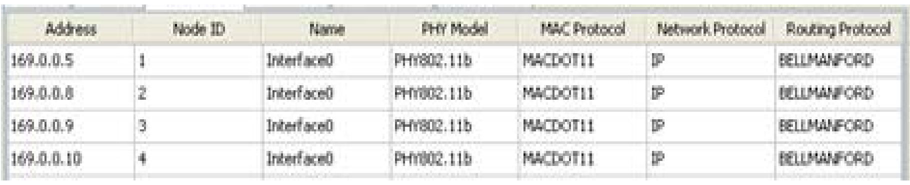


Fig. 5. Sample scenario without a DDoS Attack

The following table shows the node parameters used while simulating the scenario without an attack.

Table 1. Node parameters for a normal scenario used in Qualnet



Address	Node ID	Name	PHY Model	MAC Protocol	Network Protocol	Routing Protocol
169.0.0.5	1	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.8	2	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.9	3	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.10	4	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD

The parameters include the Logical address, ID of the Node, Interface Name, Physical Model, MAC and Internet Protocol and the Routing Table.

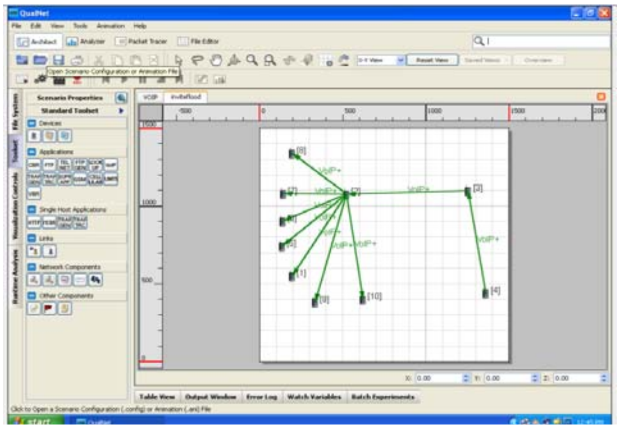
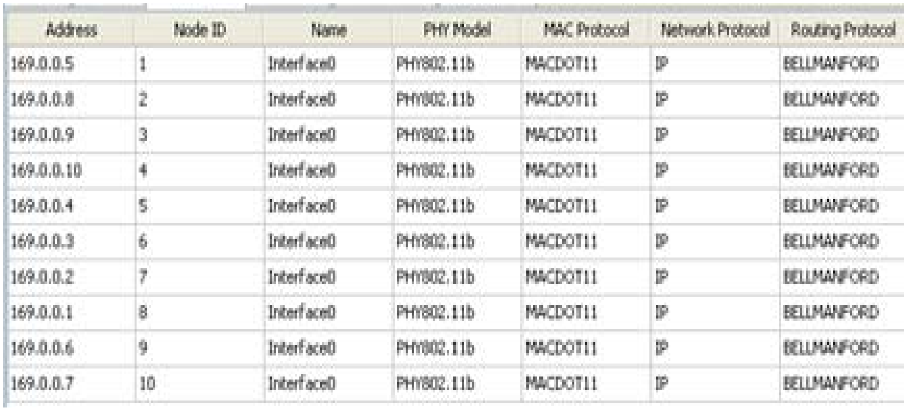


Fig. 6. VoIP Scenario with a Flooding Attack

In Fig. 5 there are four nodes, namely 1, 2, 3 and 4. Node 1 is the session initiator and node 4 is the receiver. Nodes 2 and 3 are proxy servers in 1’s and 2’s domain respectively. Node 2 (a proxy server) is the victim and it is flooded by simultaneous requests from nodes 1, 5 , 6 , 7, 8, 9 and 10. The nodes are linked using VoIP application.

The following table shows the parameters of the nodes in the attack scenario.

Table 2. Node parameters for the attack scenario used in Qualnet



Address	Node ID	Name	PHY Model	MAC Protocol	Network Protocol	Routing Protocol
169.0.0.5	1	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.8	2	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.9	3	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.10	4	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.4	5	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.3	6	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.2	7	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.1	8	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.6	9	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD
169.0.0.7	10	Interface0	PHY802.11b	MACDOT11	IP	BELLMANFORD

The traffic flow during the attack is observed in Fig. 7.

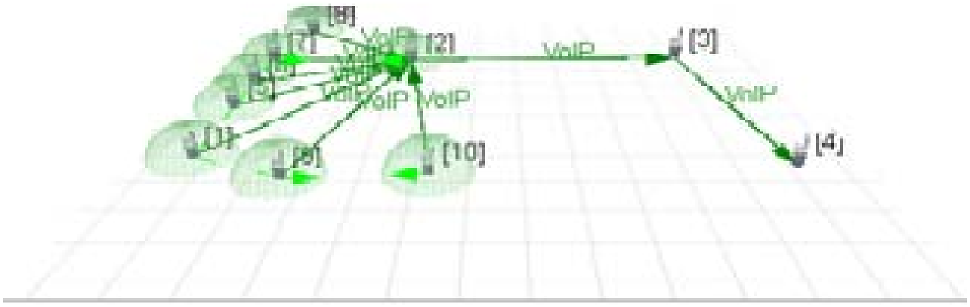


Fig. 7. Traffic flow during DDoS Attack
(node 2 is congested by the flood of messages from all the compromised nodes)

Both the scenarios are analyzed and the following graphs are obtained.

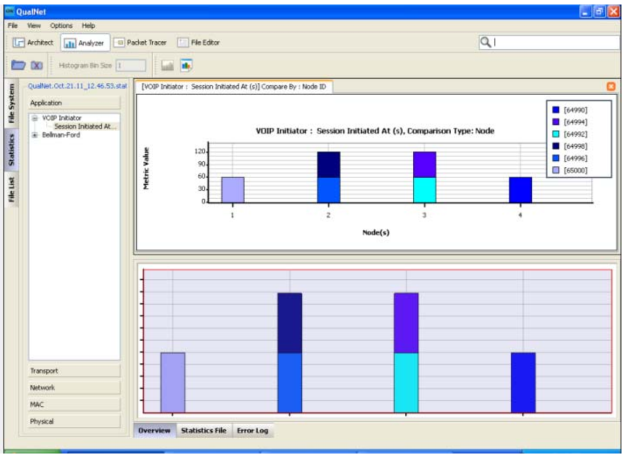


Fig. 8. Data transmission at the Application layer at nodes 1-4

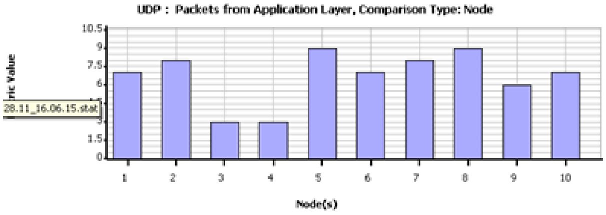


Fig. 9. Data received from the Application layer in the normal scenaio

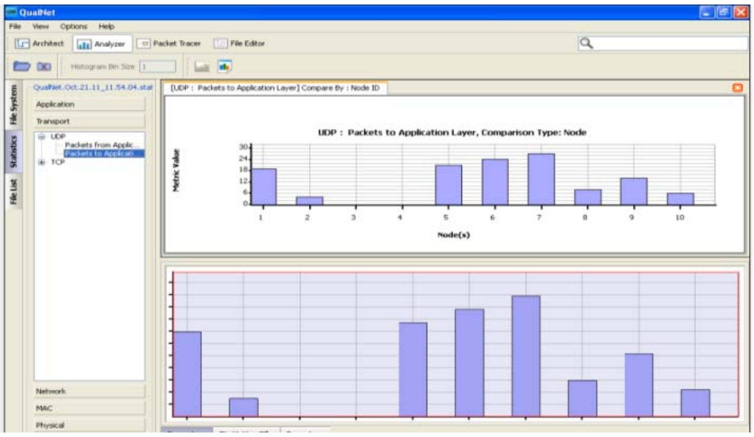
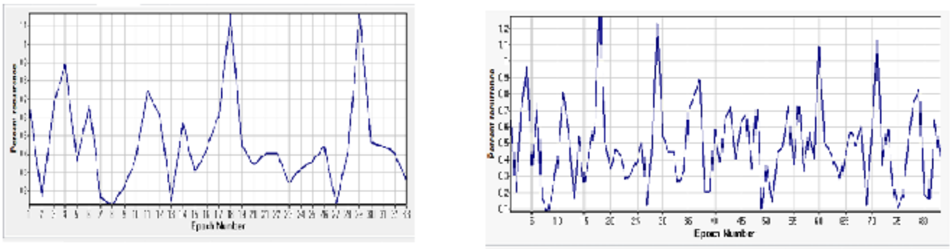


Fig. 10. Data received at the Transport layer by the UD Protocol
(no traffic at nodes 3 and 4 due to the attack)

In Fig. 9, nodes 3 and 4 receive packets from the application layer. But after the attack, as shown in Fig. 10, nodes 3 and 4 will not receive any packet from node 2 and hence they will not give any to the application layer. The Analyzer outputs (.stat files) obtained from Qualnet are given to Visual Recurrence Analysis for calculating RQA parameters. The comparison based on various parameters like divergence, recurrence rate, entropy, etc. is used to determine whether there is a DDoS attack or not.

5. Results and conclusion

The Visual Recurrence Analysis gives various graphs for both scenarios (with and without an attack). They are as follows:



(a) (b)

Fig. 11. Recurrence Rate of a normal scenario (a); Recurrence Rate of an attack scenario (b)

These graphs show the density of recurrence points in the recurrence plot in scenarios with an attack and without an attack. In the attack scenario the recurrence rate is greater as compared to the normal scenario. Recurrence means going to different states with time and coming back to the original state again. This property will be more expressed for attack the scenario since more requests are being sent to one node.

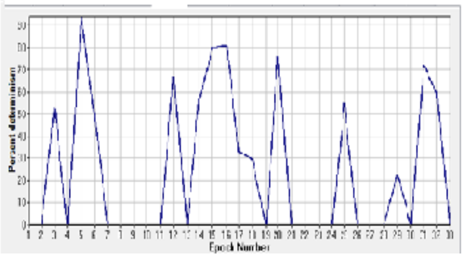


Fig. 12. Determinism of a normal scenario

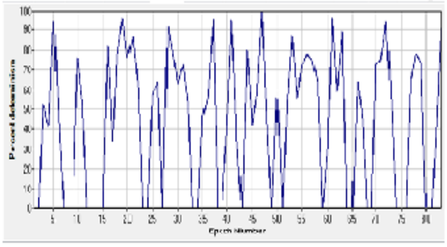


Fig. 13. Determinism of an attack

Determinism is the ratio of points forming upward diagonals to the total points in the recurrence plot. This value is set to –1 if the density of recurrence points in the recurrence plot is zero.

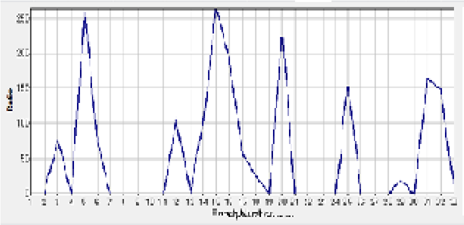


Fig. 14. Ratio of a normal scenario

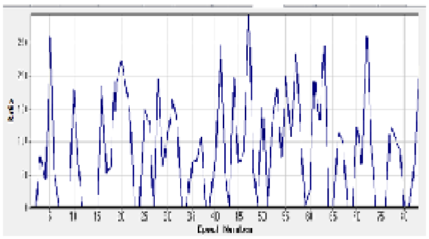


Fig. 15. Ratio of an attack scenario

These graphs show the ratio of percentage determinism to percentage recurrence. The attack scenario shows a high ratio.

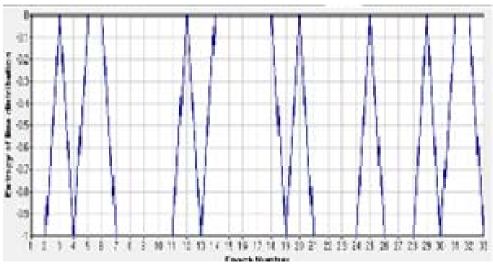


Fig. 16. Entropy of a normal scenario

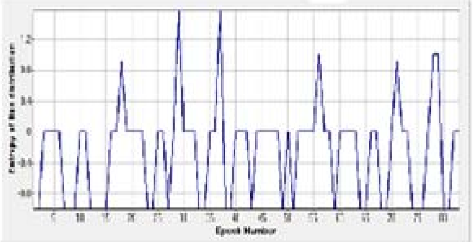


Fig. 17. Entropy of an attack scenario

Shannon’s entropy is shown here. It is the measure of uncertainty.

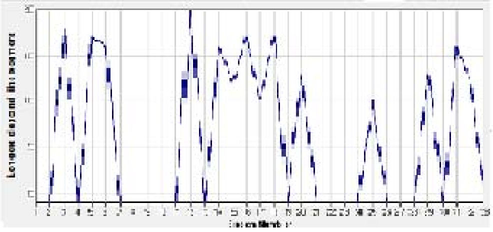


Fig. 18. Divergence of a normal scenario

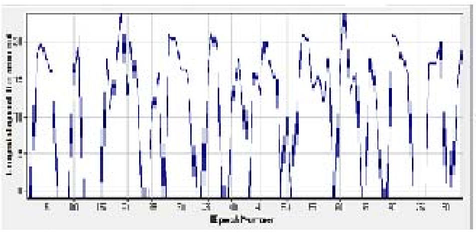


Fig. 19. Divergence of an attack scenario

These graphs show the maximal diagonal line lengths. For this purpose, the Line of Identity LOI is not taken into consideration.

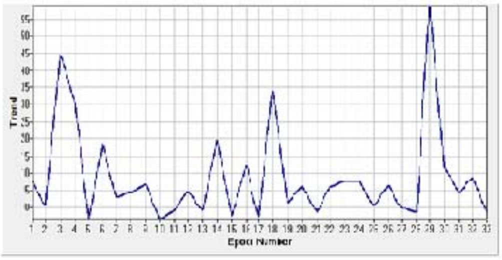


Fig. 20. Trend of a normal scenario

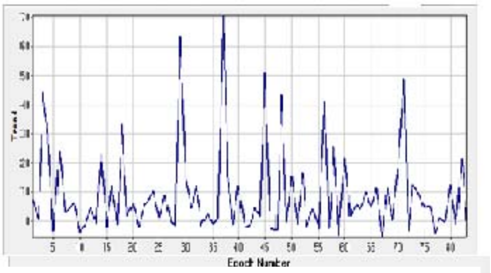


Fig. 21. Trend of an attack scenario

These graphs show the tendency of recurrence points to move away from the mean diagonal. The attack scenario tends to move away from the mean diagonal compared to the normal one.

Table 3. Comparative analysis of detection techniques

Detection techniques	Type of the Attack	Test data	**Detection results**
Activity profiling	TCP, UDP flood	6 publicly available data	**12 000 DoS attacks on 5 000 distinct victims**
Change-point detection	TCP SYNC flood attack – Constant rate	3 private network data sets	**All attacks detected**
Wavelet analysis	DoS floods		**90% anomalies detected**
Entropy based traffic mode detection	DoS/DDoS	sample data from Lincoln Lab	**99.2% of TCP SYN flooding detected**
Volume based detection techniques	DoS		**Unable to detect Short-term attacks**
Distance based detection techniques	Flooding based DDoS attacks	NS-2	**Hard to exploit in Real situation**
Network traffic based detection	DDoS	Data from Zaozhuang University with Sniffer Software	**1 out of 2 attacks were detected**
Covariance analysis model	SYN Flooding, DDoS	NS-2	**500 SYN packets/sec**
RQA BASED	**SIP based attacks**	**Qualnet**	**99.5% attacks detected**

From the observations made it is concluded that RQA is an efficient method for detecting a DDoS attack at earlier stages and thereby prevent the further effect of the attack. A profile of a normal scenario is to be maintained. The current traffic is analyzed compared with this profile. Any deviation detects the presence of an attack. This method cannot be compromised even if the attacker knows the detection scheme. In future the method will be justified by capturing live VoIP traffic.

References

1. Goode, B. Voice Over Internet Protocol (VoIP). – Proceedings of IEEE, Vol. **90**, 2002, No 9, 1495-1517.
2. Rosenberg, J., H. Schulzrinne, G. Camarillo. SIP: Session Initiation Protocol. – IETF RFC 3261, 2002.
3. Lei-Jun, L. A New Type of DDoS Defense System Study. – IEEE, 2010, 307-309.
4. Sisalem, D., J. Kuthan, S. Ehlert. Denial of Service Attacks Targeting a SIP VoIP Infrastructure – Attack Scenarios and Prevention Mechanisms. – IEEE Network, Vol. **20**, 2006, No 5, Special Issue on Securing VoIP, 26-31.
5. Jin, Shuyuan, D. S. Yeung. A Covariance Analysis Model for DDoS Attack Detection. – IEEE Communications Society, April 2004, 1822-1886.
6. Tritilanunt, S., S. Sivakorn, C. Juengjincharoen, A. Siripornpisan. Entropy-Based Input-Output Traffic Mode Detection Scheme for DoS/DDoS Attacks. – IEEE Communication Society, 2010, 804-809.
7. Lee, Je Hak, Dong Seong Kim, Sang Min Lee, Jong Sou Park. DDoS Attacks Detection Using GA based Optimized Traffic Matrix. – In: Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011, 216-220.
8. Leu, Fang-Yie, Chia-Chi Pai. Detecting DoS and DDoS Attacks using Chi-Square. – In: 5th International Conference on Information Assurance and Security, IEEE Computer Society, 2009, 255-258.
9. Nashat, D., X. Jiang, S. Horiguchi. Router Based Detection for Low-Rate Agents of DDoS Attack. – In: IEEE International Conference on High Performance Routing and Switching, 2008, 177-182.
10. Kumar, K., R. C. Joshil, Kuldip Singh. A Distributed Approach using Entropy to Detect DDoS Attacks in ISP Domain. – In: IEEE – International Conference on Signal Processing Communications and Networking, February 2007, 331-337.
11. Lam, Ho-Yu, Chi-Pan Li, S. T. Chanson, Dit-Yan Yeung. A Coordinated Detection and Response Scheme for Distributed Denial-of-Service Attacks. – IEEE Communications Society, 2006, 2165-2170.
12. Liu, Haiqin, Yan Sun, Min Sik Kim. Fine-Grained DDoS Detection Scheme Based on Bidirectional Count Sketch. – In: IEEE International Conference on Computer Communications and Networks, 2011, 1-6.
13. Chen, Chin-Ling. Detecting Distributed Denial-of-Service Attack Traffic by Statistical Test. – In: IEEE Third International Conference on Communications and Networking in China, 2008. ChinaCom 2008, 1253-1257.
14. Li, Muhai, Ming Li. A New Approach for Detecting DDoS Attacks Based on Wavelet Analysis. – In: IEEE 2nd International Congress on Image and Signal Processing, 2009, 1-5.
15. Yu, Wei, Dong Xuan, Wei Zhao. Middleware-Based Approach for Preventing Distributed Deny of Service Attacks. – In: IEEE MILCOM Proceedings, 2002, 1124-1129.
16. Nagaratna, M., V. Kamakshi Prasad, S. Tanuz Kumar. Detecting and Preventing IP-Spoofed DDoS Attacks by Encrypted Marking Based Detection And Filtering (EMDAF). – In: International Conference on Advances in Recent Technologies in Communication and Computing, IEEE 2009, 753-755.

17. Jeyanthi, N., J. Vinithra, S. Sneha, R. Thandeeswaran, N. Ch. S. N. Iyengar. A Recurrence Quantification Analytical Approach to Detect DDoS Attacks. – In: IEEE International Conference on Computational Intelligence and Communication Networks, 2011, 58-62.

18. Choi, Yang-Seo, Jin-Tae Oh, Jong-Soo Jang, Jae-Cheol Ryou. Integrated DDoS Attack Defense Infrastructure for Effective Attack Prevention. – IEEE Information Technology Convergence and Services, 2010, 1-6.

19. Tariqal, U., Y. Malikb, B. Abdulrazakb, M. Hongc. Collaborative Peer to Peer Defense Mechanism for DDoS Attacks. – In: 2nd International Conference on Ambient Systems, Networks and Technologies (ANT), 2011, 157-164

20. Siris, V. A., I. Stavrakis. Provider-Based Deterministic Packet Marking Against DDoS Attacks. – Journal of Network and Computer Applications, Vol. **30**, 2007, No 3, 858-876.

21. Park, K., H. Lee. The Effectiveness of Route-Based Packet Filtering for Distributed Denial of Attack Prevention in Power Law Internets. – In: ACM Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, 2001, 15-26.

22. Douligeris, C., A. Mitrokotsa. DDoS Attacks and Defense Mechanisms: Classification and State-of-the-Art. – Computer Networks, Vol. **44**, 2004, No 5, 643-666.

23. Du, Ping, Akihiro Nakao. OverCourt: DDoS Mitigation Through Credit-Based Traffic Segregation and Pathmigration. – IEEE Computer Communications, Vol. **33**, 2010, 2164-2175.

24. Peng, T., C. Leckie, K. Ramamohanarao. Protection from Distributed Denial of Service Using History-Based IP Filtering. – IEEE, Vol. **1**, 2003, 482-486.

25. Xiang, Yang, Wanlei Zhou. A Defense System Against DDoS Attacks by Large-Scale IP Traceback. – In: Third International Conference on Information Technology and Applications, IEEE Computer Society, 2005, 431-436.

26. Chao-Yang, Zhang. DOS Attack Analysis and Study of New Measures to Prevent. – In: International Conference on Intelligence Science and Information Engineering, IEEE, 2011, 426-429.

27. **www.xmco.fr/whitepapers/voip-security-layered-approach.pdf**

28. Jeyanthi, N., N. Ch. S. N. Iyengar. Escape-on-Sight: An Efficient and Scalable Mechanism for Escaping DDoS Attacks in Cloud Computing Environment. – Cybernetics and Information Technologies, Vol. **13**, 2013, No 1, 46-60.

29. Palmieri, F., U. Fiore. Network Anomaly Detection through Nonlinear Analysis. – Computers & Security, Science Direct, Vol. **29**, 2010, No 7, 737-755.

30. Recurrance Plots.
http://www.recurrence-plot.tk/glance.php