I J C T A, 9(41) 2016, pp. 709-716 ISSN: 0974-5572

A QUANTUM FLOW MODEL FOR RESISTING DDOS ATTACK

R.Saranya

Abstract: The Distributes Denial of Service (DDoS) attack in one the major issue in cyber security today. This cause the Internet servers being overloaded by receiving overwhelming (flooding) requests from the users. The attackers bombarded the server with unwanted traffic which prevents the legitimate user from using it. In this paper, the problem of DDoS attack is handled and security of Internet servers is maintained using Quantum Flow Model called Flooding Attack Resistance (QFM-FAR) which prevents DDoS attack by measuring the network traffic which approaches the Internet servers using the parameters like of source of origination, nature of data traffic and time duration. Then the traffic pattern model is used to measures the entropy on the test traffic data flow patterns to detect and resist the abnormal traffic flooding attack. At last the Phase Shift technique is being proposed to reveal the source data flow implicitly with an indication on origination of the abnormal flooding traffic. The heterogeneous traffic is also resisted and detected along with true positive rate, using the quantum flow resistance scheme.

Key Words: *Denial of Service attack, Flooding attack, Internet Service Provider, Quantum Flow, Fair Queuing, Traffic Pattern, Phase Shift Attack Detection*

I. INTRODUCTION

One of the major DDoS attacks that floods the network traffic and disturbs the internet services is called as the flooding attack. Many research works have been concentrated on resisting the DDoS attacks. Collaborative Protection Network against Flooding DDoS attack (CPN-F) [1] presented an intrusion prevention systems located at the Internet Service Providers using virtual protection rings. Another method called Deceiving Entropy-based DoS detection (DE-DoS) [2] provided mechanisms for vulnerability of entropy based network monitoring systems based on the incoming packet header fields and therefore degraded detection performance.

An efficient mechanism called Adaptive Selective Verification [3] ensured countermeasure to thwart DoS attacks based on timeout windows. A denial of service attack using SIM-less devices [4] was introduced to disrupt large sections of cellular network coverage. Attack Resilent Mix Zones [5] was introduced on different scale of geographic maps to prevent transition attacks. Though attacks were prevented, but the true positive rate of fair traffic patterns was compromised. This issue of true positive rate is handled in QFM-FAR scheme using Fair Queuing-based Quantum Flow model.

In recent years, mobile devices are receiving increasing amount of attentions with the increase in smart phone usages. An efficient protocol to obtain sum aggregate was presented in [6] aiming at reducing the communication overhead during the attack detection. In [7], Fault Tolerant Network interfaces were designed aiming at minimizing the faults or time taken to detect the faults using Network Interfaces. Secured data aggregation technique was introduced in [8] aiming at improving the security using iterative filtering techniques.

Distributed Token Reuse Detection [13] scheme was designed aiming at reducing the communication overhead using Distributed Privacy Preserving Access Control scheme. Optimal Distributed Malware Defence in mobile networks was designed in [14] with the objective of removing the malware infects using encounter-based distributed algorithm. In [15], detection of known and

Department of Computer Science, Central University of Tamilnadu,Thiruvarur,Tamilnadu,India
saranya@cutn.ac.in

unknown DDoS attacks using Artificial Neural Network. In [16], the vulnerabilities related to message attacks on Androids was introduced aiming in improving the detection rate.

II. PROPOSED METHOD

2.1 Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR)

In Quantum technique, any problem can be analysed in 360 degree. This model can be used for as basis for thwarting Flooding Attack Resistance (QFM-FAR), for detecting the normal and abnormal traffic data patterns with respect to user requests for resisting against the DDoS attack. The Queuing-based Quantum Flow model is designed to find and improve improving the true positive rate of patterns being generated (from normal and abnormal traffic) using source of origination, nature of data traffic and time duration. Proportional Traffic Pattern model reduces the rate of abnormal traffic being flooded Finally, Phase Shift Attack Detection improves the DDoS attack resistance rate by evaluating the mean and standard deviation)

Fair Queuing-based Quantum Flow (FQ-QF) model

Flooding attack shuts down the operation of its intended users by flooding the network traffic abnormally and disturbs the internet services rendered to users by making the service unavailable. The attack on client's resource usage is increased with more number of requests, and render the services of the legitimate client request, so client does not have direct access to the internet services. The objective of a Fair Queuing-based Quantum Flow (FQ-QF) model is measuring the network traffic approaching the internet servers. As a result an optimal true positive rate with fair traffic patterns are generated on due course of the user requests made.

The measured network traffic includes the vicinity of source (So) of origination, data traffic (D_t) when the source starts sending the data packet (P_i) and time duration (T). The data packet transmission rate is the summation of So and D_t .Let A_t be the arrival time of the data packet when it reaches on internet servers, then the arrival time for each data packet with determined source of origination is then represented as

$$A_t = \max (T (P_i) , T (So)) \quad (1)$$

From (1), the arrival time of each data packet Pi is then measured based on the maximum time it takes for a data packet to arrive at the Internet server 't' and the time for the source of origination The quantum flow measure enable the servers to identify the traffic patterns generated on due course of the user requests made.

The timestamp 'Time' of each data packet P_i residing at the head of the each queue is then compared with the timestamp for source of origination and the data packet with lowest timestamp is transmitted first.

$$\text{if } T (P_i) < T (S_0) \text{ then , Transmit } P_i \quad (2)$$

$$\text{if } T (P_i) > T (S_0) \text{ then , Do not transmit } P_i' \quad (3)$$

Input: S_o, Do , T, $P_i = P_1, P_2, \ldots, P_n$

Output: Optimal generation of fair traffic patterns

Begin: For each data packet

Measure transmission rate and arrival time

if $T(P_i) < (S_o)$ *then*

Transmit P_i

End if

if $T(P_i) > T(S_o)$ *then*

'Do not transmit P_i

End if

End for

End

Figure 1: Fair Queue Quantum (FQQ) algorithm

As shown in the Figure (1), the objective of Fair Queue Quantum (FQQ) algorithm is to provide an optimal fair traffic patterns for each data packet approaching the internet servers. For each data packet, the transmission rate and arrival time is measured based on the source of originator. Followed by this, the timestamp of each data packet with the time of source originator is compared to decide upon the data transmission. As a result, an optimal true positive rate with fair traffic patterns are generated on due course of the user requests made [15].

2.2 Traffic Pattern Model

The entropy of Traffic Pattern Model is measured on the test traffic data flow patterns and compared with training samples to detect and resist the abnormal traffic flooding attack. This in turn minimizes the rate of abnormal traffic data (i.e. data packets) being flooded. The Traffic Pattern Model is based on the assumption that under normal operations (i.e. traffic pattern), the traffic packet in one direction is proportional to the traffic packet in the opposite direction. For every source of origination 'S_o' that sends data packets 'P_i=P_1,P_2,P_n to a destination address 'S_o', the Proportional Traffic Pattern evaluates the ratio function within a pre-set time window. Let '$\alpha_{So\text{-}Sd}$' denotes the data packets sent from source of origination to the destination address and '$\beta_{So\text{-}Sd}$' denotes the data packets sent to source of origination from the destination address, then the ratio function within a pre-set time window is calculated by finding the difference source of origin from destination to the source of origin to the destination address.

The main aim of Traffic Pattern Model is that under normal operations, the number of data packets sent from the source of origination to the destination is proportional to the number of data packets sent from the destination to the source of origination, due to the proportional traffic pattern assumption. . The standard class of traffic pattern is evaluated with training sample of the previously occurred traffic in the internet servers. If a source of origination is launching a flooding attack against the target, the number of data packets sent from the source of origination will far exceed the number sent to it by the target [14].

The entropy (i.e. the ratio function) is measured on the test traffic data flow patterns and compared with training samples to detect and resist the abnormal traffic flooding attack. The Traffic Pattern Model in QFM-FAR scheme uses Kullback Leibler [1] distance measures to observe the traffic data flow patterns dissimilarity between two traffic patterns 'TP_i and TP_i`' respectively. Then relative entropy "RE' is measured on the test traffic data flow patterns and compared with training samples to detect and resist the abnormal traffic flooding attack. If the relative distributions (i.e. relative entropy)

are equivalent, the relative entropy is zero, and the more deviant the distributions are, the higher the abnormal traffic flooding attack. In this way, the entropy rate is measured.

2.3 Phase Shift Attack Detection

The quantum flow model in QFM-FAR scheme reveals the implicit source data flow and also indicates the origination (i.e. S_o ') of the abnormal flooding traffic attack being made and the time (i.e. 'T') at which it made.
The incoming data traffic patterns (IDTP) at each sample iteration is periodically measured and the phase shift values (i.e. mean and standard deviation) mean value '$mean$' and the standard deviation value 'sd' of the IDTP are computed. Let 'TP_i=TP_1, TP_2,.TP_n' represent the sample of 'n' incoming data traffic patterns measurement. Then, the mean value 'mean' and standard deviation value 'sd' of the IDTP is formulated as

$$mean = \sum_{i=1}^{n}\left(\frac{TP_i}{n}\right) \; and \; sd = \sqrt{\frac{\sum_{i=1}^{n} TP_i - mean}{n-1}} \tag{4}$$

From (4) ,If the value of standard deviation is greater than zero, then the incoming data traffic patterns are observed to come from normal flow. With the standard deviation value being less than zero, then the incoming data traffic patterns is observed to be arising from abnormal flooding traffic attack. In this way, by observing the standard deviations, normal flow and abnormal flow are measured in an efficient manner. This in turn helps in improving the DDoS attack resistance rate. Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme to resist the DDoS attack in Internet Server uses MATLAB and NS-2 The simulation setting for QFM-FAR scheme uses the NS-2 simulator with the network range of 1200*1200 m size. The number of user requests selected for experimental purpose is 70 users with 70 data packets and uses Random Way Point (RWM) model for QFM-FAR scheme [12]. The QFM-FAR scheme uses the Destination Sequence Based Distance Vector (DSDV) as routing protocol to perform the experimental work.

III. EXPERIMENTAL SETTINGS

3.1 Impact of True positive rate of fair traffic patterns

The true positive rate of fair traffic patterns being generated is the ratio of fair traffic patterns generated to the total data packets sent in the network in internet server. The mathematical formulation of true positive rate is as given below.

$$TPR = \sum_{i=1}^{n}\left(\frac{Fair\ traffic\ patterns}{DP_i}\right) * 100 \tag{5}$$

From (5), the true positive rate 'TPR' is measured based on the data packets approaching the internet servers. Higher the true positive rate, more efficient the method is said to be. The true positive rate is measured in terms of percentage (%) [15].

Table 1 True positive rate of fair traffic patterns being generated

Data Packets (MB)	True positive rate of fair traffic patterns being generated (%)		
	QFM-FAR	CPN-F	DE-DoS
7	86.13	72.48	58.32
14	88.15	77.10	62.05
21	91.32	80.27	65.22
28	86.31	75.26	62.21
35	87.19	76.14	64.09
42	85.17	74.12	62.07
49	89.37	78.32	64.27

3.2 Impact of Abnormal traffic data being flooded

In order to measure the abnormal traffic data, the number of user requests made, the data packets and the data packets size are considered. Therefore, abnormal traffic data being flooded is the product of the number of requests made with the data packets sent and the size of the data packets. The abnormal traffic data is mathematically evaluated as given below.

$$ATD = req * DP_{i} * `DP_{size} \quad (6)$$

From (6), the abnormal traffic data 'ATD' is measured using the number of user requests made 'req' is the number of data packets ' DP_i' and the size of the data packets 'DP_{size} ' respectively [7].

The targeting results of abnormal traffic data using QFM-FAR scheme is compared with two state-of-the-art methods [1], [2] for visual comparison based on the number of user requests. Our method differs from the CPN-F [1] and DE-DoS [2] in that we have incorporated Proportional Traffic Pattern Model. By applying Proportional Traffic Pattern Model in the internet servers, abnormal traffic data being flooded is analyzed by applying a within a pre-set time window. In addition, the ratio function within a pre-set time window from source of origination to the destination address and source of origination from the destination address, are considered using the Proportional Traffic Pattern Model. Therefore the abnormal traffic data flooded with data packets is reduced by 18.52% compared to CPN-F and 32.26% compared to DE-DoS respectively.

Table 2 Abnormal traffic data

Number of user requests (req)	Abnormal traffic data (packets/sec)		
	QFM-FAR	CPN-F	DE-DoS
2	85	115	131
4	98	126	135
6	115	133	155

8	129	147	167
10	137	155	175
12	148	165	172
14	155	173	195

3.3 Impact of entropy

The comparison of entropy rate is presented in table 4 with respect to different data packets in the range of 7 to 49.

Table 3 Entropy rate

Methods	**Entropy (%)**
QFM-FAR	**0.5**
CPN-F	**0.9**
DE-DoS	**1.2**

The entropy rate is improved in the QFM-FAR scheme due to the application of Phase Shift Attack Detection model. By applying Phase Shift Attack Detection model, the incoming data traffic patterns to the internet server with different traffic dimensions are measured in an efficient manner. This is because with the application of Phase Shift Attack Detection model the phase shift values (i.e. mean and standard deviation) are computed to measure the deviation from the actual on due course of the user requests made.

3.4 Impact of DDoS attack resistance rate

The DDoS attack resistance rate is the ratio of attack detected to the traffic patterns observed in a network. The mathematical formulation of DDoS attack resistance rate is as given below.

$$ARR = \sum_{i=1}^{n} \frac{Attack_d}{TP_i} * 100 \quad (7)$$

Table 4 DDoS attack resistance rate

Traffic Patterns	**DDoS attack resistance rate (%)**		
	QFM-FAR	**CPN-F**	**DE-DoS**
3	**78.13**	**64.24**	**58.13**
6	**83.44**	**67.16**	**61.25**
9	**85.14**	**72.13**	**68.31**
12	**72.13**	**68.14**	**55.24**
15	**75.89**	**72.35**	**61.32**
18	**74.21**	**70.16**	**58.21**
21	**79.32**	**74.23**	**62.31**

We consider the method with 21 different traffic patterns for experimental purpose using NS2 simulation tool.

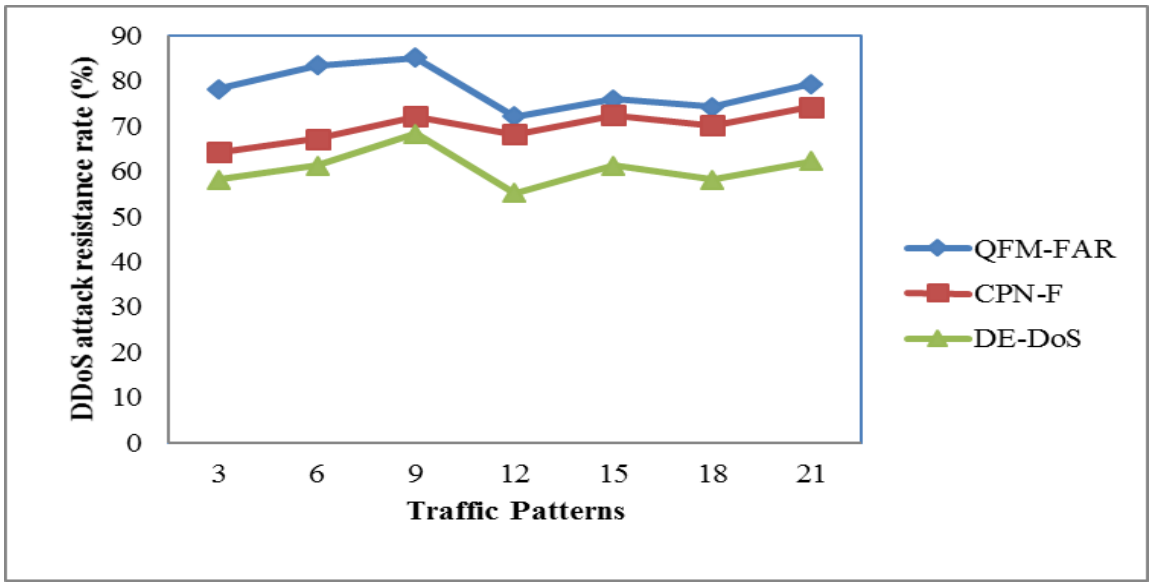

Figure 2 Measure of DDoS attack resistance rate with respect to traffic patterns

Figure 2 shows the measure of DDoS attack resistance rate with respect to differing number of traffic patterns. The DDoS attack resistance rate using QFM-FAR scheme is improved owing to the fact that the proposed scheme uses Fair Queue Quantum algorithm. With this DDoS attack resistance rate, the transmission rate, arrival time is measured in an effective manner for efficiently restricting the DDoS attack and therefore improving the DDoS attack resistance rate by 10.66% compared to CPN-F and 22.51% compared to DE-DoS respectively.

IV. CONCLUSION

In this work, an effective scheme called Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) is presented. The scheme improves the true positive rate of fair traffic patterns being generated and minimizes abnormal traffic data being flooded for efficiently restricting the DDoS attack in the internet server. The goal of Quantum Flow Modeled Flooding Attack Resistance is to restrict the DDoS attack rate using the training and test traffic data flow patterns which significantly contribute to the relevance. To do this, we first designed a Fair Queuing-based Quantum Flow model that measures the transmission rate and arrival time and estimate the fair queuing based on the Fair Queue Quantum algorithm to improve the true positive rate of fair traffic data patterns being generated. Then, based on this measure, we proposed a Proportional Traffic Pattern model for minimizing the abnormal traffic data being flooded and therefore improving the entropy rate in an extensive manner. In addition Phase Shift Attack Detection model detects the attack rate (i.e. normal or abnormal flow) on the incoming traffic data patterns and therefore ensures end to end data packet transfer for varied packets with different traffic dimensions. Through the simulations carried out using NS2, we observed that the data packet transfer provided more accurate results compared to existing methods. The results show that QFM-FAR scheme offers better performance with an improvement of true positive rate by 20.81% and reduces the abnormal traffic data by 25.39% compared to CPN-F and DE-DoS respectively.

REFERENCES

[1] Jérôme Francois, Issam Aib, and Raouf Boutaba, “FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks”, IEEE/ACM Transactions on Networking, Volume 20, Issue 6, December 2012, Pages 1 – 14.
[2] Ilker Ozcelik, Richard R. Brooks, “Deceiving entropy based DoS detection”, Elsevier, Computers & Security, Volume 48, February 2015, Pages 234–245.
[3] Sanjeev Khanna, Santosh S. Venkatesh, Omid Fatemieh, Fariba Khan, and Carl A. Gunter, “Adaptive Selective Verification: An Efficient Adaptive Countermeasure to Thwart DoS Attacks”, IEEE/ACM Transactions on Networking, Volume 20, Issue 3, June 2012, Pages 715-728.
[4] Alessio Merlo, Mauro Migliardi, Nicola Gobbo, Francesco Palmieri, and Aniello Castiglione, “A Denial of Service Attack to UMTS Networks Using SIM-Less Devices”, IEEE Transactions on Dependable and Secure Computing, Volume 11, Issue 3, May-June 2014, Pages 280-291.
[5] Balaji Palanisamy, and Ling Liu, “Attack-Resilient Mix-zones over Road Networks: Architecture and Algorithms”, IEEE Transactions on Mobile Computing, Volume 14, Issue 3, March 2015, Pages 495-508.
[6] Qinghua Li, Guohong Cao, and Thomas F. La Porta, “Efficient and Privacy-Aware Data Aggregation in Mobile Sensing”, Transactions on Dependable and Secure Computing, Volume 11, Issue 2, March/April 2014, Pages 115-129.
[7] Leandro Fiorin, and Mariagiovanna Sami, “Fault-Tolerant Network Interfaces for Networks-on-Chip”, Transactions on Dependable and Secure Computing, Volume 11, Issue 1, January/February 2014, Pages 16-29.
[8] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, and Sanjay Jha, “Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks”, IEEE Transactions on Dependable and Secure Computing, Volume 12, Issue 1, January/February 2015, Pages 98-110.
[9] Anh Le, and Athina Markopoulou, “Cooperative Defense Against Pollution Attacks in Network Coding Using SpaceMac”, IEEE Journal on Selected Areas in Communications, Volume 30, Issue 2, February 2012, Pages 442-449.
[10] Ming-Yang Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems”, Elsevier, Computer Communications ,Volume 34, Issue 1, January 2011, Pages 107–117.
[11] Gianluca Dini, Angelica Lo Duca, “Towards a reputation-based routing protocol to contrast black holes in a delay tolerant network”, Elsevier, Ad Hoc Networks, Volume 10, Issue 7, September 2012, Pages 1167–1178.
[12] Noel De Palma, Daniel Hagimont, Fabienne Boyer, and Laurent Broto, “Self-Protection in a Clustered Distributed System”, IEEE Transactions on Parallel and Distributed Systems, Volume 23, Issue 2, February 2012, Pages 330 – 336.
[13] Rui Zhang, Yanchao Zhang, and Kui Ren, “Distributed Privacy-Preserving Access
Control in Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems, Volume 23, Issue 8, August 2012, Pages 1427-1438.
[14] Yong Li, Pan Hui, Depeng Jin, Li Su, and Lieguang Zeng, “Optimal Distributed Malware Defense in Mobile Networks with Heterogeneous Devices”, IEEE Transactions on Mobile Computing, Volume 13, Issue 2, February 2014, Pages 377-391.
[15] Alan Saied , Richard E. Overill , Tomasz Radzik, “Detection of known and unknown DDoS attacks using Artificial Neural Networks”, Elsevier, Neuro computing, 8 August 2015, Pages 1 – 9.
[16] Khodor Hamandi, Alaa Salman, Imad H. Elhajj, Ali Chehab, and Ayman Kayssi, “Messaging Attacks on Android: Vulnerabilities and Intrusion Detection”, Hindawi Publishing Corporation, Mobile Information Systems, Volume 2015, February 2014, Pages 1 – 14.
[17] Douglas C. MacFarland, Craig A. Shue(B), and Andrew J. Kalafut, “Characterizing Optimal DNS Amplification Attacks and Effective Mitigation”, Springer, Pages 15 – 27.
[18] Imrul Kayes, “A Survey on Privacy and Security in Online Social Networks”, ACM Computing Surveys Template, Pages 1-40.
[19] http://www.darkreading.com/vulnerabilities-and-threats/2016-ddos-attack-trends-by-the-numbers/d/d-id/1326754
[20]] https://threatpost.com/arbor-ddosattacks-getting-bigger-as-reflectionincreases/108752.
[21] Kreutz , Diego , Fernando MV Ramos , Paulo Esteves Verissimo , Christian Esteve Rothenberg , Siamak Azodolmolky , and Steve Uhlig . “ Software-defined networking: A comprehensive survey ”. Proceedings of the IEEE 103 , no. 1 (2015): 14 – 76 .
[22] Mehdi Sookhak, Adnan Akhundzada, Alireza Sookhak,Mohammadreza Eslaminejad, Abdullah Gani, Muhammad Khurram Khan, Xiong Li, Xiaomin Wang, “Geographic Wormhole Detection in Wireless Sensor Networks”, Geographic Wormhole Detection in Wireless Sensor Networks, 2015, Pages 1-21.