International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 23 (2015) pp 43484-43491

An Efficient DDOS Traffic Flooding Attack Resistance Model Using Quantum Flow

R. Saranya[1], Dr. S. Senthamarai Kannan[2]

[1]Assistant Professor, Dept. of CSE, Pannai College of Engineering and Technology
Affiliated to Anna University-Chennai, Manamadurai Main Road Sivagangai-630561, Tamilnadu, INDIA saranyarajiakodi@gmail. com
[2]Professor, Dept. of CSE, Pandian Saraswathi Yadav Engineering College Affiliated to Anna University-Chennai, Arasanoor, Thirumansolai Post Sivagangai-630561, Tamilnadu, INDIA stanfordssk@gmail. com

ABSTRACT
With huge demand on internet services being rendered by large application server, Denial of Service (DoS) attack becomes a key security issue in the network service provisioning. Many current DDoS attack model for preventing flooding attack in the Internet Service Provider has been presented. In this work we address the problem of DDoS attack and maintain the security of internet servers using Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme. The QFM-FAR scheme efficiently restricts the DDoS attack in the internet servers. In QFM-FAR scheme, Fair Queuing-based Quantum Flow model measures the network traffic approaching the internet servers with the vicinity of source of origination, nature of data traffic and time duration. Next, the Proportional Traffic Pattern model in QFM-FAR scheme measures the entropy on the test traffic data flow patterns and compared with training samples to detect and resist the abnormal traffic flooding attack. Finally, the Phase Shift Attack Detection in QFM-FAR reveals the implicit source data flow and also indicates the origination of the abnormal flooding traffic attack being made and the time at which it made. The experimental evaluation is conducted with KDD CUP 2012 data set for the proposed QFM-FAR scheme and compared with the existing state of art methods. The cross traffic is also resisted and detected with the quantum flow model on the incoming data traffic patterns to the server with different traffic dimensions. Simulations carried out on the proposed scheme have produced results that demonstrate effectiveness of the proposed attack resistance scheme in terms of number of user requests, true positive rate, abnormal traffic data being flooded, entropy rate and DDoS attack resistance rate.

Key-words- Denial of Service attack, Flooding attack, Internet Service Provider, Quantum Flow, Fair Queuing, Proportional Traffic Pattern, Phase Shift Attack Detection

1 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.
In [9], Spacemac was used against pollution attacks to significantly lower the communication overhead. Prevention for selective black hole attacks was introduced in [10] using Anti Black Hole mechanism. However, the vulnerability of abnormal traffic being flooded was not solved. In this paper we propose a solution by introducing Proportional Traffic Pattern Model that reduces the rate of abnormal traffic being flooded in the internet server. A reputation-based protocol for attack resistance in delay tolerant network (DTN) was introduced in [11]. The method used acknowledgement, node lists and aging to thwart black holes in DTN. A firewall-based intrusion detection system was introduced in [12] with the objective of detecting the known and unknown attacks using self protected system.
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 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. Optimal amplification attacks was designed in [17] aiming at improving the attack detection rate using query rate limiting. In [18], a survey on preventing DDoS attacks in social networks was presented. Geographic wormhole detection [19] in sensor networks was designed using pair wise key pre-distribution technique. Mechanisms for detection and defence against backbone web traffic were presented in [20].

In this paper, we propose a Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme and thoroughly compare their performance with regard to abnormal traffic data, true positive rate, DDoS attack resistance rate and entropy rate. This is achieved using an integrated fair queuing-based quantum flow and proportional traffic pattern model. Detailed performance evaluations confirm the efficacy and efficiency of the proposed QFM-FAR scheme in thwarting DDoS attacks in internet servers, which makes QFM-FAR scheme practical solution for efficiently restricting the DDoS attacks.

The remainder of this paper is organized as follows. Section 2 describes the problem statement and the assumptions and presents our novel robust scheme for restricting the DDoS attack in the internet server. Section 3 describes our experimental results. Section 4 presents the discussion with the parametric definitions using the table form and graph. Finally, the paper is concluded in Section 5.

2 Design of Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme

In this section, the design of Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme aiming at improving the true positive rate of fair traffic patterns being generated by reducing the rate of abnormal traffic data being flooded is presented. The normal and abnormal traffic data patterns with respect to different number of user requests is designed to detect the DDoS attack resistance rate. The Quantum Flow Modeled Flooding Attack Resistance includes three parts. The first part, Fair Queuing-based Quantum Flow model is designed with the objective of improving true positive rate of fair patterns being generated using source of origination, nature of data traffic and arrival time. The second part, Proportional Traffic Pattern model minimizes the rate of abnormal traffic being flooded with the aid of the transmission rate and arrival time. Finally, Phase Shift Attack Detection improves the DDoS attack resistance rate by evaluating the phase shift (i. e. mean and standard deviation).

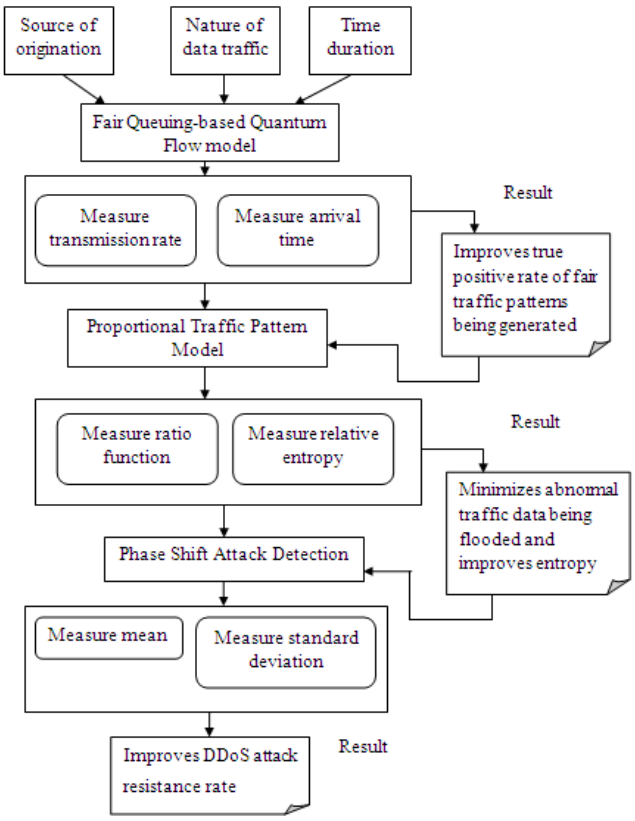

Fig. 1 Block diagram of Quantum Flow Modeled Flooding Attack Resistance scheme

2. 1 Design of Fair Queuing-based Quantum Flow model

DoS attack makes the network resources temporarily or permanently deny the services provided to the users. Flooding attack is one of the major DoS attacks which floods the network traffic abnormally and disturbs the internet services rendered to users. Denial of service attack flooding misinterprets the user requests and makes the network service disable to permit traffic. The attack on client's resource usage is increased with more number of requests, and the client does not have direct access to the internet server services.

In this section, we first briefly design a Fair Queuing-based Quantum Flow (FQ-QF) model with the objective of measuring the network traffic approaching the internet servers. The measured network traffic includes the vicinity of source of origination (i. e. '$Source_o$'), nature of the data traffic (i. e. ' DT_{nature}'), and time duration (i. e. '$Time$').

The structure of network traffic used for the fair queuing-based quantum flow model is shown in Fig. 2.

Source of origination '$Source_o$'	Nature of data traffic ' DT_{nature}'	Time duration '$Time$'

Fig. 2 Structure of network traffic

From the Fig. 2, '$Source_o$' denotes the source of origination, ' DT_{nature}' denotes the nature of data traffic or the traffic

patterns when the source starts sending the data packet 'DP_i', and '$Time$' denotes the time when router starts sending the data packets to the internet servers. If 'DT_{nature}' is expressed in terms of how many clock ticks it takes to transmit the data packet 'DP_i', then the mathematical formulation of data packet transmission rate is as given below

$$\text{Transmission}_{\text{rate}} = \text{Source}_o + \text{DT}_{\text{nature}} \quad (1)$$

Let '$Arrival_t$' represents 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 given below

$$\text{Arrival}_t = \text{MAX}(\text{Time}(\text{DP}_i), \text{Time}(\text{Src}_o)) \quad (2)$$

From (2), the arrival time '$Arrival_t$' of each data packet 'DP_i' is then measured based on the maximum time it takes for a data packet to arrive at the internet server '$Time\ (DP_i)$' and the time for the source of origination '$Time\ (Source_o)$'. 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 'DP_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.

$$\text{If Time}(\text{DP}_i) < \text{Time}(\text{Source}_o) \text{ then Transmit DP}_i \quad (3)$$

$$\text{If Time}(\text{DP}_i) > \text{Time}(\text{Source}_o) \text{ then}$$
$$\text{Do not Transmit DP}_i \quad (4)$$

Input: source of origination '$Source_o$', Data traffic nature 'DT_{nature}', Time '$Time$', Data Packet '$DP_i = DP_1, DP_2, \dots, DP_n$'
Output: Optimal generation of fair traffic patterns (i. e. improved true positive rate)
Step 1: Begin Step 2: For each data packet DP_i Step 3: Measure transmission rate using (1) Step 4: Measure arrival time using (2) Step 5: If $Time\ (DP_i) < Time\ (Source_o)$ Step 6: Then '$Transmit\ DP_i$' Step 7: End if Step 8: If $Time\ (DP_i) > Time\ (Source_o)$ Step 9: Then '$Do\ not\ transmit\ DP_i$' Step 10 :End if Step 11:End for Step 12: End

Fig. 3 Fair Queue Quantum (FQQ) algorithm

As shown in the Fig. 3, 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.

2. 2 Proportional Traffic Pattern Model

The standard class of traffic pattern is evaluated with training sample of the previously occurred traffic in the internet servers using the Proportional Traffic Pattern Model. The entropy of Proportional 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 Proportional 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 '$Source_o$' that sends data packets '$DP_i = DP_1, DP_2, \dots, DP_n$' to a destination address '$Source_d$', the Proportional Traffic Pattern evaluates the ratio function within a pre-set time window.

Let '$\alpha_{Source_{o\_}Source_d}$' denotes the data packets sent from source of origination to the destination address and '$\beta_{Source_{d\_}Source_o}$' denotes the data packets sent to source of origination from the destination address, then the ratio function within a pre-set time window is mathematically formulated as given below

$$\text{Ratio function} = \left(\frac{\alpha_{Source_{o\_}Source_d}}{\beta_{Source_{d\_}Source_o}}\right) \quad (5)$$

The objective behind Proportional 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. 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 Proportional 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. The Kullback Leibler entropy is then formulated as

$$\varphi_i = \left(\frac{TP_i}{TP_i'}\right) \quad (6)$$

From (6), the relative entropy to detect and resist the abnormal traffic flooding attack is then formulated as given below

$$\text{RE}(\text{TP}_i, \text{TP}_i') = \sum_{i=1}^{n} TP_i * \varphi_i \quad (7)$$

From (7), the 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. With the application of Kullback Leibler distance measures, the entropy rate is found to be less that shows that abnormal traffic data being flooded is reduced in a significant manner. Fig. 4 given below shows the Kullback Leibler Distance-based Proportional Traffic Pattern algorithm.

Input: data packets from source of origination to destination '$\alpha_{Source_o\_Source_d}$', data packets from destination to source of origination '$\beta_{Source_d\_Source_o}$', Traffic Patterns '$TP_i and\ TP_i'$'
Output: Minimized abnormal traffic flooding attack rate
Step 1: Begin Step 2: For each data packets Step 3: Measure the ratio function using (5) Step 4: Evaluate Kullback Leibler entropy using (6) Step 5: Measure relative entropy using (7) Step 6: If $RE = 0$ Step 7: Normal traffic flow Step 8: End if Step 9: If $RE > 0$ Step 10: Abnormal traffic flooding attack Step 11: End if Step 12: End for Step 13: End

Fig. 4 Kullback Leibler Distance-based Proportional Traffic Pattern algorithm

As shown in the Fig. 4, the Kullback Leibler Distance-based Proportional Traffic Pattern algorithm includes three steps. For each data packets, the ratio function within a pre-set time window, the proportional traffic patterns are measured. Followed by this, the Kullback Leibler relative entropy between two traffic patterns is measured. Finally, based on the relative entropy value, normal traffic flow and abnormal traffic flooding attack is differentiated where when the relative distributions are equivalent, the relative entropy is zero denoting the normal flow pattern. On the other hand, more deviant the distributions, higher the abnormal traffic flooding attack is said to be. In this manner, by applying Kullback Leibler distance measures, entropy rate is improved reducing the abnormal traffic data being flooded.

2. 3 Phase Shift Attack Detection

Finally, the Phase Shift Attack Detection model detects the attack rate (i. e. normal or abnormal flow) on the incoming traffic data patterns to the server with different traffic dimensions. The quantum flow model in QFM-FAR scheme reveals the implicit source data flow and also indicates the origination (i. e. '$Source_o$ ') of the abnormal flooding traffic attack being made and the time (i. e. '$Time$') 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 '$TP_i = TP_1, TP_2, \dots, TP_n$' 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 given below

$$mean = \sum_{i=1}^{n} \left(\frac{TP_i}{n}\right) \quad (8)$$

$$sd = \sqrt{\frac{\sum_{i=1}^{n} TP_i - mean}{n-1}} \quad (9)$$

From (8) and (9), mean '$mean$' and standard deviation 'sd' for incoming data traffic patterns are measured. 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.

3 Experimental settings

Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme to resist the DDoS attack in Internet Server uses MATLAB and NS-2 simulator. The mathematical formulation in QFM-FAR scheme is evaluated using MATLAB and the results are applied in NS-2 simulator for conducting simulation settings. 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. The QFM-FAR scheme uses the Destination Sequence Based Distance Vector (DSDV) as routing protocol to perform the experimental work.

The QFM-FAR scheme's moving speed in the network is about 6 m/s for each user requests with a simulation rate of 40 milliseconds to perform single data packet transfer from source to destination node through intermediate nodes. The values of each parameter for performing experiments are shown in Table 1. Experiment is conducted on the factors such as true positive rate of fair traffic patterns being generated, abnormal traffic data being flooded, entropy and DDoS attack resistance rate with respect to the user requests. The results of the metrics of QFM-FAR scheme are compared against the existing methods such as Collaborative Protection Network against Flooding DDoS attack (CPN-F) [1] and Deceiving Entropy-based DoS detection (DE-DoS) [2].

Table 1 Simulation setup

PARAMETER	VALUE
Protocols	DSDV
Network range	1200 m * 1200 m
Simulation time	40 ms
Mobility model	Random Way Point
Number of nodes	10, 20, 30, 40, 50, 60, 70
Network simulator	NS 2. 34
Network load	4 packets/sec
Mobility speed	6 m/s
Pause time	10 s

4 Discussion

The performance of Quantum Flow Modeled Flooding Attack Resistance (QFM-FAR) scheme is compared with the existing Collaborative Protection Network against Flooding DDoS attack (CPN-F) [1] and Deceiving Entropy-based DoS detection (DE-DoS) [2]. The performance is evaluated according to the following metrics.

4. 1 Impact of True positive rate of fair traffic patterns being generated

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.

$$TPR = \sum_{i=1}^{n} \left(\frac{Fair\ traffic\ patterns}{DP_i} \right) * 100 \quad (10)$$

From (10), 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 (%).

Table 2 Tabulation for 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

The Table 2 represents the true positive rate obtained using NS2 simulation and comparison is made with two other methods, namely CPN-F [1] and DE-DoS [2]. To conduct experiments, data packet is in the range of 7 MB to 49 MB was considered. Fig. 5 shows the result of true positive rate versus the varying data packets. To better perceive the efficacy of the proposed QFM-FAR scheme, substantial experimental results are conducted and illustrated in Figure 5. The QFM-FAR scheme is compared against the existing CPN-F [1] and DE-DoS [2].

Results are presented for different number of data packets. Higher, the number of data packets, more successful the method is. The results reported here confirm that with the increase in the number of data packets, though the increasing rate of true positive rate is not linear, however betterment achieved using QFM-FAR scheme. The process is repeated with number of data packets ranging from 7 MB to 49 MB for conducting experiments. As illustrated when compared to two other methods CPN-F [1] and DE-DoS [2], the QFM-FAR scheme had better changes using the extensive Fair Queuing-based Quantum Flow model. This is because in order to obtain better true positive rate, fair queuing is measured to determine based on the timestamp that results in the improvement of true positive rate. Furthermore, based on the transmission rate and arrival time of data packets, the timestamp for source of origination and the data packet is compared, with the lowest timestamp being transmitted first which in turn improves the true positive rate by 13. 04% compared to CPN-F and FIPP and 28. 58% compared to DE-DoS.

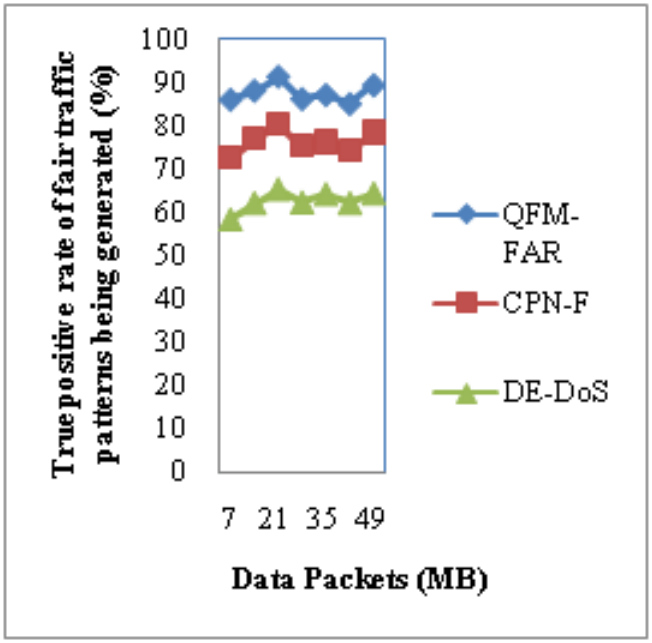

Fig. 5 Measure of true positive rate with respect to data packets

4. 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.

$$ATD = req * DP_i * DP_{size} \quad (11)$$

From (11), the abnormal traffic data 'ATD' is measured using the number of user requests made 'req', number of data packets 'DP_i' and the size of the data packets 'DP_{size}' respectively.

Table 3 Tabulation for 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

In order to decrease the abnormal traffic data being flooded at the internet server with respect to the number of user requests, the rate of abnormal traffic data using the QFM-FAR scheme and the two methods, CPN-F and DE-DoS are presented with visual comparison is presented in table 3. The results for 14 different user requests are illustrated in f Fig. 6. The abnormal traffic data being flowed with respect to user request using our

scheme QFM-FAR offer comparable values than the state-of-the-art methods.

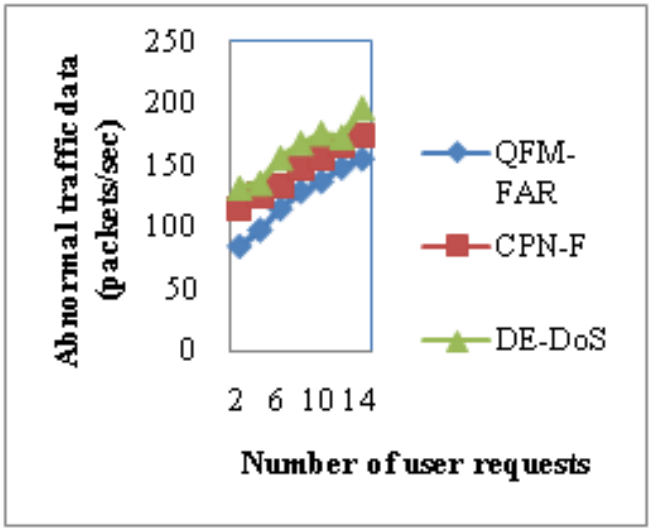

Fig. 6 Measure of abnormal traffic data with respect to number of user requests

The targeting results of abnormal traffic data using QFM-FAR scheme is compared with two state-of-the-art methods [1], [2] in figure 6 is presented 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.

4. 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 4 Tabulation for entropy rate

Methods	Entropy (%)
QFM-FAR	0. 5
CPN-F	0. 9
DE-DoS	1. 2

Fig. 7 given below shows the entropy rate in the internet server for efficiently restricting the DDoS attack using QFM-FAR scheme, CPN-F [1] and DE-DoS [2] versus increasing number of data packets in the range of 7 to 49.

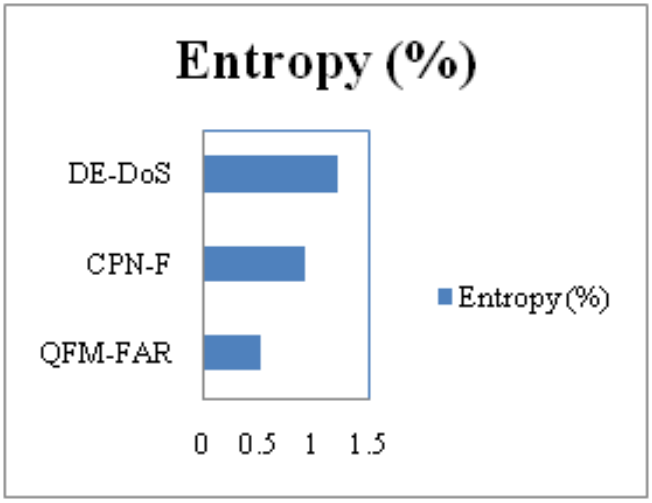

Fig. 7 Measure of entropy rate

From Fig. 7, it is illustrative that the entropy for efficiently restricting the DDoS attack is improved using the proposed scheme QFM-FAR. 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. Therefore, the entropy rate is reduced using the QFM-FAR by 80% compared to CPN-F and reduced by 33. 33% compared to DE-DoS respectively.

4. 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.

$$ARR = \sum_{i=1}^{n} \frac{Attack_d}{TP_i} * 100 \quad (12)$$

From (12) the attack resistance rate 'ARR' is measured using the attack being detected, '$Attack_d$' and the traffic patterns 'TP_i' observed during single iteration. Higher the DDoS attack resistance rate more efficient the method is said to be.

Table 5 Tabulation for 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

The DDoS attack resistance rate for QFM-FAR scheme is elaborated in table 5 and comparison made with two other methods CPN-F and DE-DoS respectively. We consider the method with 21 different traffic patterns for experimental purpose using NS2 simulation tool. The following Fig. 8 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.

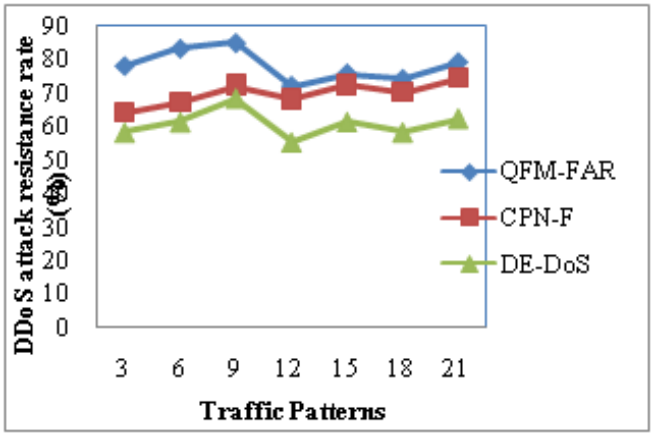

Fig. 8 Measure of DDoS attack resistance rate with respect to traffic patterns

5 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] 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, January 2015, Pages 1-21.

[20] Wei Zhoua, Weijia Jia b, Sheng Wenc, Yang Xiang c, Wanlei Zhouc, "Detection and defense of application-layer DDoS attacks in backbone web traffic", Elsevier, Future Generation Computer Systems, Volume 38, September 2014, Pages 36-46.