QVMMA : A Short term and Long Term Layer 3 DDoS Detector and Mitigator

Sonia Laskar
MTech Student,
Comp Engg Dept. ,
NMIMS MPSTME Mumbai

Dhirendra Mishra, PhD
Associate Professor,
Comp Engg Dept. ,
NMIMS MPSTME, Mumbai

ABSTRACT
Distributed Denial of Service (DDoS) attacks continue to harm servers using intense wars against popular ecommerce and content websites. The short term and long term types of popular DDoS attacks can be detected, prevented and mitigated using the proposed novel Qualified Vector Match and Merge Algorithm (QVMMA) in real time. 14 feature components are used to generate an attack signature in real time and stored in dynamically updated DDoS Captured Attack Pattern (DCAP)[30]database. It is effective in detecting new and old attacks. Persistent DDoS attacks cause financial damage or reputation loss by loss of the company's valuable clients. The server's availability is heavily compromised. Popular websites Github and BBC UK faced DDoS attacks in 2015. Long term DDoS attack directed on Github continued for over 118 hours[34,35]. Short term DDoS attack experienced by BBC[36] website caused its patchy response. The main crux of the problem is the absence of a way to differentiate between attack records and legitimate records while the attack is occurring in real time. Several methods[1-31,37-42,43] are listed in brief in the paper. Post mortem solutions are not applicable in real time. Available real time solutions are slow. QVMMA is an ideal faster real time solution to prevent DDoS attacks using Statistical Feature Vector Generation. Matlab is used for DDoS real time simulation where the topologies (bus, star, abilene network) are created using OMNET++[33]. QVMMA generates and uses Statistical Feature Vector for Attack Signature Generation, Matching and Identification only for qualifier satisfied records. The web server's log files used as input to QVMMA are according to W3C log format standard[34]. Experimentation is completed with exhaustive 336 cases. Four networks are tested with 5, 8, 10, 13 nodes. Performance evaluation of QVMMA concludes EER is 11.8% when threshold is 1.6. Using model of FAR and FAR, the trendline provides threshold at 1 with EER at 10%. Abilene network achieves best result. As the number of attackers, nodes and intermediate routers increase, detection time increases. If threshold is increased, the accuracy reduces. If the number of nodes increases, accuracy increases. Thus it is concluded that QVMMA can be used for effective layer 3 DDoS Prevention and Mitigation in real time based on results generated in Matlab simulation. Extended results are provided. A model is provided in this paper to predict the detection time for any number of attackers. Other models are provided based on data collected through experimentation to formulate a relation between detection time, accuracy, Actual Attack Traffic Passed Rate (A_ATPR) with respect to the number of attackers. The corresponding correlation coefficient and regression coefficient are calculated to identify and conclude the strong relationships. This paper focuses on results and discussion on studying the effects and trend observed based on increasing the number of attackers during a DDoS attack. Thus QVMMA is fast enough to be used in real time to detect and mitigate short term or long term layer 3 Denial of Service(DoS) and more complex DDoS attacks.

Keywords
DDoS, DoS,QVMMA, Matlab, OMNET++

1. INTRODUCTION
Distributed Denial of Services (DDoS) is an illegal online web attack where the attacker uses coordinated botnet, an army of 'zombies' to compromise the availability of victim server by flooding[11,12] it with innumerable requests beyond server's capacity. This layer 3 attack is very easy to conduct as many DDoS attack tools available in dark web. DDoS attacks are very difficult to detect as actual attacker conceals itself behind the set of innocent 'zombies' who may be unaware that a large scale attack is being launched on victim server through them. These innocent 'zombies' are secondary victims but the primary main victim is the targeted server. The crux of problem is absence of a way that can effectively differentiate between the legitimate records and illegitimate or attack packets in real time. QVMMA provides such a distinction between legitimate and illegitimate packets. Feature vector can be effectively used to detect and identify DDoS attack records at different layers. The attack records that are identified are dropped for preventive mitigation of DDoS attack on victim. One in five companies worldwide become a DDoS attack victim. Such attacks remain active causing prolonged damage from a few hours to several weeks. Deccan Chronicle[34,35], dated April 29, 2015, reported above statement as conclusion of Kaspersky Lab's and B2B's international survey with categorizing two types of DDoS attacks: "a powerful short term attack or persistent long running campaign". Both the short term and long term types of popular DDoS attacks can be detected, prevented and mitigated using the proposed novel Qualified Vector Match and Merge Algorithm (QVMMA) in real time. QVMMA algorithm proposed is tested in this paper can be used to prevent DDoS attacks before they harm the target victim server. The different techniques available for DDoS detection is listed in section 2. This paper discusses the QVMMA algorithm for DDoS detection and mitigation. QVMMA is a novel technique proposed in this paper with 14 feature components. Matlab simulation is used to test the proposed algorithm on simulated network created in OMNET++.

2. LITERATURE SURVEY
Existing classification of techniques and systems for DDoS solutions distinguished based on deployment location and basic concept[1-30,43] used to detect DDoS attacks are listed in Fig. 1. Solution can be pre or post mortem. Proposed QVMMA is pre mortem real time which can be implemented as a host based solution and it can be extended to be implemented as network based solution for better results. Statistical methods are simpler and faster in real time as compared to other available methods in literature survey. There can be 3 types of DDoS attacks based on the layer in the TCP/IP networking stack the DDoS attack is directed upon. They are : Layer 3, Layer 4 and Layer 7. Next Section 3

discusses QVMMA algorithm.

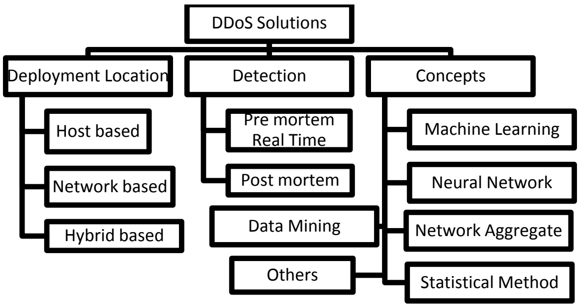

Figure 1 : Different Traffic Anomaly detection methods available in literature[1-30, 43]

3. QVMMA ALGORITHM

QVMMA stands for Qualified Vector Match and Merge Algorithm used for DDoS detection and mitigation in real time. The steps in QVMMA algorithm[43]can be divided into 2 sequences. Sequence 1 is for training the DCAP database and sequence 2

Sequence 1: Online Generate Attack Vectors from DDoS attacks to store and train DCAP database:

1. Run the Matlab simulation for DDoS attack to identify Attack Vectors or Attack signatures in real time. Program randomly selects the source port address, data packet or payload size. Random number of virus generated requests with random number of legitimate requests are generated by simulation.
2. Derive the feature components fc1, fc2, fc3….fcn where n=14.
3. Create feature vector FV from above components: FV={fc1,fc2,fc3,fc4……fcn}
4. Create feature vector characterizing each attacker (may differ for each tool): A1, A2,A3……..An.
5. Create General Attack Vector(GAV) which serves as a summary for DDoS attack and it is derived from the above set of attackers
6. Store them in DCAP (DDoS Captured Attack Pattern) database.

Sequence 2: Online Deduplication steps based on Statistical Feature Vector Generation to test:

1. Store N records in a temporary file. N is determined based on the number of attacks detected in the previous stage.
2. Start Stage 1 at victim server or it can be placed at edge router. Generate Qualifiers Q={Q1,Q2} for each flow identified based on Source IP address and Destination IP address.
3. Use Qualifiers to qualify as suspicious records for those records which satisfy the Qualifier Condition QC where [p α (1/H)].
4. Calculate feature components fc1,….., fcn where n=12 of suspicious flows .
5. Generate Feature Vector FV={fc1,fc2,……….fcn} for each suspicious flow.
6. Calculate the similarity measure E using Normalized Absolute Distance between the GAV and FV using Eqn(1):
   a. E=[(GAV)-(FV)]/FV (1)
7. If E > T_GAV, then it is an Attack. Else it is not an attack
8. If E > T_GAV, then determine the similarity measure S between FV and different attack signatures A1,…..An stored in DCAP using formula in Eqn (2):
   a. S = [(An)-(FV)]/ FV (2)
9. If Sn of FV matches Threshold T_S partially or completely, then the attacker is An.
10. Else FV is a new pattern of DDoS attacker from a new attacker.
11. Hence identify FV as An+1 and store it in updated DCAP.
12. Remove the duplicate requests from attackers and drop any other incoming requests from that ip address.
13. Next, use the source IP address from the above generated feature vector After second attempt of DDoS attack from the same source IP address, then block that particular ip address. It can be used to determine its binder detection used to identify its previous history of attacks, if any.
14. Request for a Virus Scan.
15. Follow step 6 again.

4. EXPERIMENTAL EVALUATION PARAMETERS AND SETTING

Networks, number of nodes, number of legitimate clients and attackers, thresholds are varied to test the algorithm. Number of nodes considered are: 5,8,10,13. Number of victims is limited to 1 in this Matlab simulation. Topologies considered shown in Fig.2 are: Bus, Star and Abilene network. grantThresholds gT ={1,2,3} are used.

4 simulated networks created in OMNET++ and tested in Matlab simulation are shown in Fig.2:

1. Straight Single Path Bus Bus1 shown in figure 2(a)
2. Dual Path Bus called Bus2 shown in figure 2(b)
3. Star Topology shown in figure 2(c)
4. Abilene Network shown in figure 2(d)

All possible configurations tested are used for experimentation. 28 such unique combinations or configurations (called code) for each above network is provided. Calculation of Total number of test cases is denoted by T.

T = Total number of configuration * Total number of networks * Total number of grantThresholds (3)

T = (28) * 4 * 3 = 112 + 112 + 112 = 336 cases

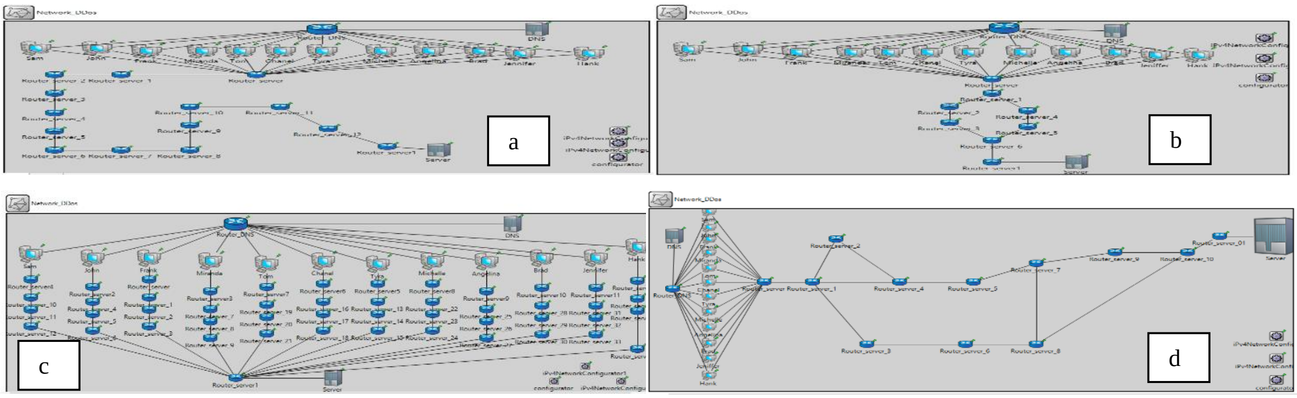

Figure 2. Networks[43] simulated in OMNET++ for testing with 13 nodes containing 12 clients and 1 victim server. (a)Straight bus ;(b) Bus 2 dual path Network ;(c) Star Network ;(d) Abilene Network

Table 1. Average Accuracy, Detection Time, A_ATPR, Average of GAR and GRR for each code averaged at Threshold={1,2,3}

Code	Average Acc	Number of A	Number of Legitimate	Victim Count	Total Nodes	Detection Ti	A_ATPR (%	Average of G
1	90.3179874	1	3	1	5	0.893673	74.62671	91.41331
2	78.2186863	2	2	1	5	0.997448	85.74922	82.57491
3	79.0179378	3	1	1	5	1.410851	90.40397	82.16511
4	89.3887211	1	6	1	8	0.998517	74.83417	91.31647
5	82.0102418	2	5	1	8	1.122488	82.19094	85.65945
6	80.7281237	3	4	1	8	1.080474	85.23946	84.13626
7	84.8018994	4	3	1	8	1.2533	88.86485	86.02559
8	85.3122628	5	2	1	8	1.862361	92.62469	85.96258
9	85.9921472	6	1	1	8	1.742391	93.0446	86.22
10	84.4104613	1	8	1	10	1.014168	67.1142	87.93008
11	85.4270702	2	7	1	10	1.003257	77.32931	88.97918
12	84.3796501	3	6	1	10	1.051532	87.9255	87.52023
13	82.5524441	4	5	1	10	1.274457	90.31347	86.00628
14	83.6815288	5	4	1	10	1.521056	89.64025	85.71424
15	84.4862347	6	3	1	10	1.906458	91.12004	86.11588
16	85.6238619	7	2	1	10	1.634034	91.86955	85.96241
17	84.2272833	8	1	1	10	1.642446	92.50361	81.36443
18	90.143804	1	11	1	13	0.486671	69.24902	92.48245
19	87.1820253	2	10	1	13	0.587816	79.76405	90.09554
20	84.7657732	3	9	1	13	0.918791	85.04457	88.49626
21	88.0312446	4	8	1	13	1.266406	87.09518	89.4434
22	87.1161816	5	7	1	13	1.277021	88.7635	88.62497
23	85.2782294	6	6	1	13	1.627694	89.12544	87.67532
24	86.7712415	7	5	1	13	2.018514	90.66856	87.57575
25	85.4659117	8	4	1	13	2.246167	91.69495	86.5077
26	85.6919756	9	3	1	13	2.481634	91.31844	84.09255
27	86.3850502	10	2	1	13	2.625544	92.79003	85.86025
28	85.9272355	11	1	1	13	3.221902	92.16286	85.31256
Average	85.1191148					1.470253	86.18111	86.82976

Table 2. Comparison of Average of Performance Evaluation Metrics at gT={1,2,3}

Sr.No.	Fields in Performance Evaluation File	Meaning	gT={1}	gT={2}	gT={3}
1	Grant_Threshold	Grant Threshold	1	2	3
3	Code	Code	1-28	1-28	1-28
4	Topology/ Networks	Network	1-4	1-4	1-4
5	Detection Time (secs)	Detection Time	1.69	1.45	1.245
6	GRR (%)	Genuine Rejection Rate	92.8	85.4	73.6
7	GAR (%)	Genuine Acceptance Rate	69.6	99.3	100
8	FRR (%)	False Rejection Rate	30.37	0.7	0
9	FAR (%)	False Acceptance Rate	7.19	14.61	26.4
10	A_ATPR (%)	Actual_ Attack Traffic Passed Rate	13.424	14	14.1
11	A_LTPR (%)	Actual_ Legitimate Traffic Passed Rate	86.58	86	85.9
12	E_ATPR (%)	Experimental_ Attack Traffic Passed Rate	16.37	27	36.64
13	E_LTPR (%)	Experimental_ Legitimate Traffic Passed Rate	83.6	73	63.4
14	Dev_ATPR (%)	Deviation in Attack Traffic Passed Rate Detected	-2.9	-12.6	-22.5
15	Dev_LTPR (%)	Deviation in Legitimate Traffic Passed Rate Detected	+2.9	12.6	22.5
16	Accuracy (%)	Accuracy	90.39	87.3	77.48
17	Average of GAR and GRR (%)	Average of GAR and GRR	81.2	92.35	86.81

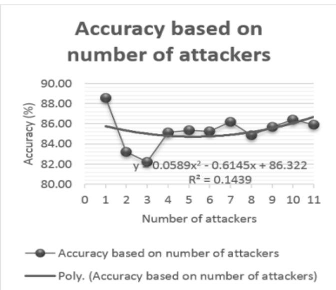

Figure 8(a) : Poly: Accuracy based on number of attackers of atta ers

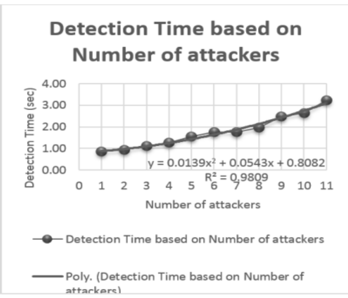

Figure 8(b):Poly: Detection Time based on number

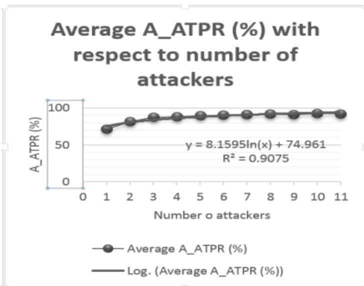

Figure 8(c) : Log: A_ATPR based on number of attackers attack

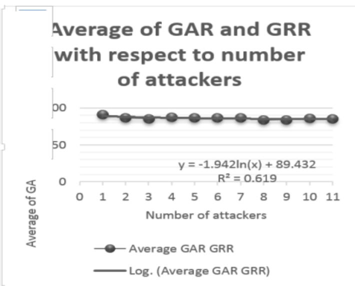

Figure 8(d) : Log: Average GAR GRR based on

Figure 3 : Graph of Accuracy, Detection Time, Average ATPR, Average of GAR and GRR with respect to Number of attackers

5. RESULTS AND DISCUSSION

The Table 1 provides the performance evaluation results wrt. Code, average accuracy, number of attackers, legitimate clients, victim count, total nodes, detection time, A_ATPR, Average of GAR and GRR. As per above Table 2, as grant threshold gT is increased : following metrics increase across the three thresholds :GAR, FAR, A_ATPR, E_ATPR, Dev_LTPR. Following metrics decrease across the three thresholds :Detection time, GRR, FRR, A_LTPR, E_LTPR, Accuracy, Dev_ATPR, Average of GAR and GRR.Although GAR increases, but the overall accuracy of the system decreases if the threshold in increased. Following Figure 4 is plotted using the above Table 2, the Equal Error Rate (EER) obtained graphically from experimental data is 12% at threshold of gT=1.6, that is gT can be between 1 and 2 using the data obtained from experimentation.

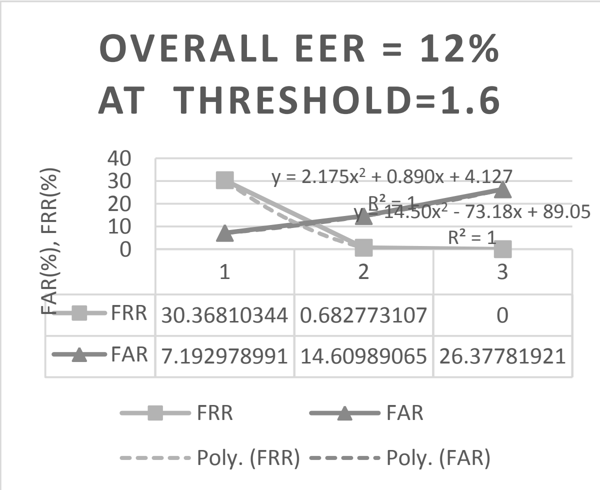

Figure 4: Overall EER Obtained is 12% at threshold = 1.6

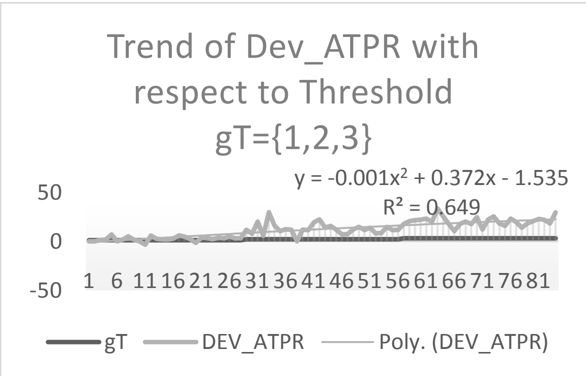

Figure 5 : Trend of Dev_ATPR w.r.t Threshold

The polymorphic equations of FAR and FRR obtained using Figure 4 are represented in Table 3. Since regression coefficient R2 is 1, the equation represented in Table 3 covers 100% of the points from graph. Using these mathematical model obtained from above equations represented in Table 3 , the calculated values of EER is 10% at threshold of 1 from above graph as these values can be observed in Figure 4 dotted trendlines. Using Figure 5, the general trend of Dev_ATPR increases with the increase in threshold. Also, the average Dev_ATPR is 2.44% at threshold 1, Dev_ATPR is 12.55% at threshold 2 and Dev_ATPR is 20.44% at threshold 3. Thus the minimum Dev_ATPR obtained is at threshold 1. Thus threshold gT selected should be 1 for better overall performance of the system.

Table 3. Best Fitting Model for FAR and FRR

Metrics	R^2	Polymorphic Equation
FAR	1	$y = 2.1755x^2 + 0.8904x + 4.1271$
FRR	1	$y = 14.501x^2 - 73.189x + 89.056$

Table 4 provides the performance evaluation results obtained based on the number of attackers. Based on the simulation done in Matlab, Average accuracy is 85.35 %. Accuracy differs due to testing done at different thresholds and different topology. Detection Time increases as the number of attackers increase as the number of records to be processed in the web server log increases. Detection Time will also increase if the number of routers increase between the attacker and web server. As the number of attackers increase, the Actual Attack Traffic Generated also increases, A_ATPR or Actual Attack Traffic Passed Rate increases and A_LTPR, Actual Legitimate Traffic Passed Rate increases.

Table 4. Average Accuracy, Detection Time, A_ATPR, Average of GAR and GRR with respect to number of attackers from 1 to 11

No. of attackers	Accuracy (%)	Detection Time(sec)	Average A_ATPR(%)	Average GAR GRR(%)
1	88.56524	0.848257271	71.45602	90.78558
2	83.20951	0.92775225	81.25838	86.82727
3	82.22287	1.115412042	87.15338	85.57947
4	85.12853	1.264721084	87.82952	87.15842
5	85.36999	1.553479306	89.5309	86.76726
6	85.2522	1.758847361	90.5134	86.6704
7	86.19755	1.760080361	91.26905	86.76908
8	84.8466	1.969042028	92.09928	83.93606
9	85.69198	2.481634083	91.31844	84.09255
10	86.38505	2.625544333	92.79003	85.86025
11	85.92724	3.221902083	92.16286	85.31256

From Table 5, it can observed that Accuracy has a weak positive correlation with the number of attackers during a DDoS attack. Average of GAR and GRR has negative correlation with the number of attackers but better than accuracy's correlation with number of attackers. Detection Time and Average A_ATPR has strong positive correlation with number of attackers. Thus Detection time and Average A_ATPR increase as the number of attackers increase. Detection Time and Average A_ATPR can be modelled using the polymorphic equations and logarithmic equation stated in row 2 and 3 respectively as these performance metric values can be accounted for 98.09% and 90.75% times as regression coefficient is maximum at 0.9809 and 0.9075. The plotting of experimental data and the trendline with the maximum R2 obtained for accuracy, Detection Time, Average A_ATPR and Average of GAR and GRR with respect to number of attackers as shown in Table 5 is plotted in Figure 3. Based on Figure 3, table 5 is tabulated. Thus the equation generated for detection time (Table 5, 2nd row) can be used to predict the amount of time taken for x substituted with n number of attackers during DDoS attack. Based on this equation, this QVMMA algorithm can detect upto 63 attackers in less than a minute. Under 2 minutes, it can detect upto 90 attackers. Under 21 minutes, it can detect upto 300 attackers.

Table 5. Best Fit Model Equations for 4 Performance Evaluation Metrics

Sr. No.	Number of attackers with respect to	Coefficient of correlation : r	Coefficient of Regression : R^2			Rank	Maximum R^2	Best Fit Model Equation
			Linear Equation	Polynomial Equation	Logarithmic Equation			
1	Accuracy	0.185994	0.0346	**0.1439**	0.0002	4	0.1439	$y = 0.0589x^2 - 0.6145x + 86.322$
2	Detection Time	0.975465	0.9515	**0.9809**	0.7769	1	0.9809	$y = 0.0139x^2 + 0.0543x + 0.8082$
3	Average A_ATPR	0.814644	0.6636	0.9073	**0.9075**	2	0.9075	$y = 8.1595\ln(x) + 74.961$
4	Average of GAR and GRR	-0.69063	0.477	0.5731	**0.619**	3	0.619	$y = -1.942\ln(x) + 89.432$

6. CONCLUSION

QVMMA is useful for layer 3 DDoS flooding attack, the most popular and is easy to conduct using DDoS attack tools. Every DDoS attack tool will have its own attack signature as will every client and attackers have. This can be used to identify from when and where a DDoS attack is being conducted. It differentiates it with flash crowd and DDoS attack. Filtering stage QVMMA for statistical feature vector generation. Qualifiers qualify and differentiate between the records that are normal or suspicious attack packets. The Qualifiers Entropy and Probability save time and memory which otherwise may have been consumed to generate feature vector for all records. The multiple features used for derived generation of statistical feature vector are source ip address, source port address, destination ip address, destination port address, page requested and payload or data size of packets, timestamp of packets received at server. These are in accordance with W3C log formats standard for server logs. Random payload and random of requests are generated with random port addresses for simulation of attackers. QVMMA is fast enough to be implemented in real time with the available ip records.

Use of more feature components will increase time required for signature computation, thus number of feature vector components selected is a tradeoff between preferable maximum accuracy, minimum detection time, minimum FAR, minimum FRR, maximum GAR, maximum GAR. Time taken to detect attack is a critical component in saving the target victim server from any damage. Lesser the time taken to detect the DDoS attack, lesser is the probability of damage caused by attack. This can be determined using experimentation. The main aim of ‘QVMMA for DDoS Prevention/Protection and Mitigation Services’ is to prevent a DDoS attack while it is occurring in real time, expanding from the mere post mortem analysis which is static. This simulation prototype created in Matlab demonstrates dynamically creating an online real time database Distributed Capture Attack Pattern(DCAP) while attack is occurring in Sequence 1 for training the reference database of attack signatures. Sequence 2 tests the signatures created dynamically in real time on a new set of records generated real time in Matlab. Performance evaluation metrics, its extended results and discussion are provided.

Performance evaluation of QVMMA algorithm based on experimental data concludes that EER is 11.8% when threshold is 1.6. Error is below 12 % when threshold used is 2 or less than 2 when tested in Matlab simulation. Performance evaluation of QVMMA algorithm based on trendline determined based experimental data provides EER as 10% with threshold is 1. Deviation in ATPR or Dev_ATPR detected is 2.44% at threshold of 1. Abilene network achieves best results. As the number of attackers and intermediate routers between the server and client increases, detection time increases. As threshold is increased, the accuracy reduces. As number of nodes increases, accuracy and detection time increases. Number of nodes includes number of attackers as well as legitimate clients and victim server. As number of attackers increase, accuracy, detection time, actual attack traffic passed rate increases. Thus QVMMA can be used for effective DDoS Prevention and Mitigation in real time with a greater number of nodes with any topology. QVMMA is fast enough to counter real time layer 3 flooding DDoS attacks in real time. Thus QVMMA can be used to increase resilience against long term and short term DDoS attacks in real time.

7. REFERENCES

[1] Yang Xiang, Wanlei Zhou. Mark-Aided Distributed Filtering by Using Neural Network for DDoS Defense. IEEE Globecom 2005.

[2] Jose Anand, K. Sivachandar. Performance Analysis of ACO-based IP Traceback. International Journal of Computer Applications (0975-8887), December 2012; Volume 59-No.1.

[3] V. Paruchuri, A Durresi, S Chellappan. TTL based Packet marking. IEEE 2008.

[4] S Mishra, R. K. Pateriya. Mitigating DDoS using Threshold-based Filtering in Collaboration with Capability Mechanisms. International Journal of Computer Applications(0975-8887), June 2014; Volume 96-No.10.

[5] Arun Kumar, Sai Ashritha. Analysis of various IP traceback techniques- A Survey. IJCA(0975-8887), September 2013; Volume 77-No.13, pp.13-16.

[6] Ruiliang Chen, Jung-Min Park, Randolph Marchany. A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks. IEEE Transactions On Parallel And Distributed Systems, May 2007; Volume. 18, NO. 5.

[7] Sriharsha Gangam, Puneet Sharma, Sonia Fahmy. Pegasus: Precision Hunting for Icebergs and Anomalies in Network Flows. Proceedings IEEE INFOCOM, 2013.

[8] S Ranjan, R. Swaminathan, M Uysal, A Nucci, E Knightly. DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks. IEEE/ACM Transactions on Networking, February 2009; Vol. 17, No. 1.

[9] M Tavallaee, Wei Lu, Shah Iqbal, Ali A. Ghorbani . A Novel Covariance Matrix based Approach for Detecting Network Anomalies. IEEE 2008 ; 978-0-7695-3135-9.

[10] Wei Xiong, Naixue Xiong, Laurence T. Yang, Jong Hyuk Park, Hanping Hu, Qian Wang. An anomaly-based detection in ubiquitous network using the equilibrium state of the catastrophe theory. Published online: Springer Science Business Media, LLC 5 July 2011.

[11] Shuyuan Jin, Daniel S. Yeung. A Covariance Analysis Model for DDoS Attack Detection. IEEE 2004.

[12] A. Chonka, J. Singh, W. Zhou. Chaos Theory Based Detection against Network Mimicking DDoS Attacks. IEEE COMMUNICATIONS LETTERS, September

2009; VOL. 13, NO. 9.

[13] G. Zhang, Manish Parashar. Cooperative Defence against DDoS Attacks. Journal of Research and Practice in Information Technology February 2006 ; Vol. 38, No. 1.

[14] Rui Zhong, Guangxue Yue. DDoS Detection System Based on Data Mining. Proceedings of the Second International Symposium on Networking and Network Security (ISNNS ’10) Jinggangshan, P. R. China, 2-4, April. 2010; pp. 062-065.

[15] Andreas Kind, Marc Ph. Stoecklin, Xenofontas Dimitropoulos. Histogram-Based Traffic Anomaly Detection. IEEE Transactions On Network Service Management JUNE 2009; VOL. 6, NO. 2.

[16] Shui Yu, Wanlei Zhou, Robin Doss. Information Theory Based Detection Against Network Behaviour Mimicking DDoS Attacks. IEEE COMMUNICATIONS LETTERS, April 2008; VOL. 12, NO. 4.

[17] S Gupta, D Grover, A Bhandari. Detection Techniques against DDoS Attacks: A Comprehensive Review. International Journal of Computer Applications (0975 – 8887) June 2014; Volume 96– No.5.

[18] S Zargar, J Joshi, D Tipper. A Survey of Defence Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, FOURTH QUARTER 2013; VOL. 15, NO. 4.

[19] Stoecklin, Marc P., Le Boudec, Jean-Yves, Andreas K. Detection Technique Based on Multi-modal Flow Behaviour Models. PAM 2008 LNCS Springer Verlag 2008 ; 4979, p. 212-221.

[20] S Siraj, A K Gupta, R. Badgujar. Network Simulation Tools Survey. International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, June 2012; Issue 4,ISSN : 2278 – 1021.

[21] V Mishra, S Jangale. Analysis and comparison of different network simulators. International Journal of Application or Innovation in Engineering & Management (IJAIEM), Special Issue for International Technological Conference 2014; ISSN 2319 – 4847.

[22] Yu Chen, Kai Hwang, Wei-Shinn Ku. Collaborative Detection of DDoS Attacks over Multiple Network Domains. IEEE Transactions On Parallel And Distributed Systems June 2007; TPDS-0228-0806.

[23] http://www.calyptix.com/2014/03/top-threats-massive-denial-of-service-attacks/

[24] computerworld-nsl@idgindia.net

[25] Jérôme François, Issam Aib, Raouf Boutaba. FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. IEEE/ACM TRANSACTIONS ON NETWORKING, December 2012 ; VOL. 20, NO. 6.

[26] Q Jiang, Y Jing, X Xiao, X Wang. A Coding-Based Incremental Traceback Scheme against DDoS Attacks in MANET. Communications and Network, Scientific Research Journal, September 2013; 5, 478-484.

[27] CERT Coordination Center. Denial of Service Attacks. January 3, 2000. Available from URL: <http://www.cert.org/tech_tips/denial_of_service.html>[January 3, 2000]

[28] N. Samaan, A. Karmouch. Network anomaly diagnosis via statistical analysis and evidential reasoning. Network and Service Management, IEEE Transactions June 2008; vol. 5, no. 2, pp. 65–77.

[29] S. G. Mallat. A theory for multi-resolution signal decomposition: the wavelet representation. Pattern Analysis and Machine Intelligence, IEEE Transactions 1989; vol. 11, no. 7, pp. 674–693.

[30] Sonia Laskar, Dr. Dhirendra Mishra. A Survey on traffic anomaly detection methods used to detect DDoS attacks. ICTTM IIT Delhi 11-12th April 2015 ;ISBN : 9780992680053.

[31] M Karim Aroua, BZouari. A distributed and coordinated massive DDOS attack detection and response approach. IEEE 36th International Conference on Computer Software and Applications Workshops, IEEE, 2012.

[32] Server Log Standard Format. Available from URL: http://www.w3.org/Daemon/User/Config/Logging.html

[33] Thomas Chamberlain. Learning OMNET++. Packt Publishing, 2013.

[34] Gopinathan K, Practice Head for Managed Security and Network Services, Wipro, in conversation with CIO&Leader. DDoS attacks and how to protect enterprises from it. December 12, 2013. Source Online Available from URL: http://www.cioandleader.com/articles/38859/indian-firms-still-not-prepared-to-fight-ddos-attacks/.

[35] One in five DDoS attacks last for days even weeks. Deccan Chronicle, April 29,2015, 15.55pm IST. Available from URL: www.deccanchronicle.com/150429/technology-latest/one-five-ddos-attacks-last-days-or-even-weeks/.

[36] Web attack knocks BBC websites offline. 31 December, 2015. Available from URL: http://www.bbc.co.uk/news/technology-35204915.

[37] Method and system for protecting against denial of service attacks using trust, quality of service, personalization and hide port messages. US 20070266426 A1

[38] Handling of DDoS attacks from NAT or proxy devices. US Patent US8370937B2.

[39] Jung-Taek Seo, KiWook Sohn, Eungki Park. DDoS Flooding Attack response approach using deterministic push back method. US Patent US20080127324A1. May 29, 2008.

[40] Anand Eswaran, S Guntupallia. Distributed Denial of Service Signature Transmission. US Patent US20100212005A1. Aug. 19, 2010.

[41] Thomas Wittenschlaege. Vector based Anomaly detection. US Patent US008683591B2. Mar. 25, 2014.

[42] Detecting Application Layer DDoS Attacks. China Patent CN102638474B.

[43] Sonia Laskar, Dr. Dhirendra Mishra, ‘Qualified Vector Match and Merge Algorithm (QVMMA) for DDoS Prevention and Mitigation’, ICCCV 2016, Mumbai, Elsevier Journal, Procedia Computer Science (2016) , 79C, pp. 41-52.