International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Reroute the Packets After Finding Zombie using DPM Techniques

S. Suresh, N. Sankar Ram

Abstract—In recent days there are several problems are raised in different servers which are connected through online. These servers are dedicatedly meant to provide a specific web services to the various clients connected to it. These servers are maintained for government purposes as well as private organizations. When certain application are being developed to run in above servers are not attributed to security issues in early development stages. DDoS attack is one among in various security threads. The attack which meant for above criteria is known as Distributed Denial of Service attack. DDoS is happening due to dropped packets and requests were obtained by others instead of actual legitimate user. Many solutions are discussed in various research article and currently available in market to solve such attacks. Few improvement is required in evaluation metrics such as scalability, working mode, Storage etc..We proposed a new mechanisms in DPM called DS-DPM to improve DPM techniques in scalable issues because many DPM mechanism are yielding better result but when number of nodes in existing network suddenly increases day by day the performance of DPM is degrading slower than previous network structure.

Keywords—DS-DPM, DDoS attacks, Servers, Scalability, Performances

I. INTRODUCTION

A mechanism to fix the access and exit points or various routes of DDoS affected traffic forwarding packets into and out of current setup domain names is discussed. We look at valid origin addresses found by way of routers from test sample visitors under non-attack situations. under affected conditions, we aimed to hit upon path difficulties via mentioning out which routers have been utilized for illegitimate supply information, to arrange the attack paths. Then recollect installing nodes troubles and display outcomes from test simulations to prove the possibility of our implementation. They focused to enforce specified Trace back procedure in a language and more sensible experiments and results are carried out. The experiments shows that accurate outgoing flows, with huge traceback speed of some seconds, are achieved. when comparing to existing techniques, our new dissimilar approach is non-intrusive, no longer needed any changes to the internet routers and different packets. unique actual facts relating to the attack isn't necessary permitting a broad type of DDoS attack discovery strategies for use. The victim is also reassured from the traceback undertaking all through an attack. The scheme is easy and competent, permitting for a rapid traceback, and scalable due to the giving out of dispensation workload[1][2]

Recently, DDoS attack discovery metrics are purposely alienated into two classes: the signature-primarily based measurement and anomaly-primarily based measurement. The signature-based metric strongly depends upon on expertise that deploys a predefined locate of assault signatures all along with styles or Strings as signatures to competition inward packets. the anomaly-primarily based detection metric typically models the usual group of people (traffic) behavior and deploys it to appraise differences with inward set of connections behavior. Anomaly-based discovery has many obstacles. First, in anomaly-based discovery systems, attackers can educate discovery structures to increasingly recognize irregularity community performance as regular. 2nd, the false elevated quality charge by means of the anomaly-based completely discovery metric is normally better than the one the bring into play of the signature-based detection metric. it is hard-hitting to set the correct thresholds which assist to equilibrium the counterfeit wonderful rate and the bogus terrible rate. 1/3, it's miles very tough to extract the features of normal and anomalous group of people behaviors exactly. An anomaly-based discovery metric uses a predefined only one of its kind threshold, such as an strange divergence of a few statistical individuality from ordinary society visitors, to choose out odd traffic in the middle of all normal visitors. consequently, the usage and preference of statistical methods and gear is crucially necessary . it's miles usually typical that the incomplete Gaussian din trait may be used to reproduce real society guests in aggregation and the Poisson allocation feature can be used to reproduce the DDoS assault interchange in aggregation[3]-[9]

Even though software program-defined networking (SDN)brings more than a few compensation through decoupling the influence flat surface from the proceedings plane, there may be a opposing association in the middle of SDN and distributed denial-of-provider (DDoS) attacks. On single hand, the competencies of SDN build it even to find out and to act in response to DDoS assaults. at the dissimilar hand, the division of the administer plane from the in order aircraft of SDN introduces innovative attacks.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
S. Suresh*, Research Scholar, Department of Information Technology, Faculty of CSE , Sathyabama Institute of Science and Technology Rajiv Gandhi Salai, Jeppiaar Nagar, Chennai, Tamil Nadu 600119, India and AP/CSE, Panimalar Engineering College, Chennai Tamil Nadu , India
N. Sankar Ram , Professor, Department of Computer Science and Engineering, Rajalakshmi Engineering College Rajalakshmi nagar, Thandalam, Chennai, Tamil Nadu , India

consequently, SDN itself may be a objective of DDoS attacks. on this dissertation, Their primary talk the brand new trends and character of DDoS attacks in cloud computing environments. They show that SDN brings us a novel hazard to defeat DDoS attacks in cloud computing environments, and sum up right capabilities of SDN in defeating DDoS assaults. Then they discussed and general idea the studies in the region of initiation DDoS attacks on SDN and the techniques in resistance to DDoS attacks in SDN. similarly, they analyzed a number of difficult situations that would like to be addressed to alleviate DDoS associated in SDN with cloud computing. This paintings can help take in for questioning the way to build full use of SDN's advantages to overcome DDoS assaults in cloud computing environments and how to save you SDN itself from rotating keen on a sufferer of DDoS assaults.[10]-[12]

II . METHODS OF DPM

The mechanisms are used in the direction of place assaults are 1.Proactive 2.Reactive three, Survival. wherein outline again method of internet protocol is comes underneath immediate system. Reactive mechanism is the method wherein it is feasible to become aware of the attacks subsequent to it's miles exaggerated especially injured party.

The DDoS attacks provide discovery is enormously tough because it's followed through extra horizontal retailers,zombies and hackers so we decisive to propose upper answer that be supposed to no longer harm the legal individual at any cost and their presentation also be measured. IP hint again mechanisms are used to recognize the provider of attackers specifically probabilistic packet marking scheme(PPM) in addition to deterministic packet marking scheme(DPM). PPM system inscription each small package while it is forwarding to every one of the routers with accurate identifier in IP field while DPM inscription the packets in way out router handiest. in spite of the fact that PPM performance may be used to stagger on after and before assault establish in network. DPM move toward is extra suitable to locate assault in DoS though it needs in addition improvement to notify the attacks in DDoS attack.

We strong-minded to employ deterministic packet marking format in planned method to find out DDoS attacks. To mixture the problem they get better primary DPM approach to a hash trait to provide digests or Hash values of way in cope with. They future each packets belonging to way in interface on edge router express a a small number of hash cost. Hash feature is used to authenticate the authentication procedure in provide and break spot .DPM method was used together with hash mark but it leads added transparency in group of people presentation. Every the present strategies PPM (probabilistic packet marking) and DPM (deterministic packet marking) necessitate routers to bring in marks into man or woman packets. So it's miles memories –extensive. moreover, the PPM approach can handiest perform in a close by variety of the net (ISP network) in which the protector has the power to influence. but, this appearance of ISP network is normally attractive small, and we can't trace back to the assault possessions located out of the ISP community.

The DPM approach requires every one the internet routers to be up to date for small package marking. but, with the majority effectual 25 spare bits to behave in as IP small package, the scalability of DPM is a large difficulty. furthermore, the DPM mechanism poses an huge task on garage for packet classification for routers. therefore, it's miles infeasible in put into practice at nearby. DPM mechanism must be augmented dependable with approach across attacks in DDoS environment. We planned DS-DPM technique to detect DDoS assaults subsequent verifying the guests capability surrounded by the group of people.

III. IMPLEMENTATION AND RESULTS

We have simulated our implementation in NS2 and obtained results to meet the constraints given in the abstract. Now we start from mathematical notation followed by algorithm and other details of implemented result. Consider the R1 and R5 are egress router and installed with DS-DPM implementation to Monitor the malicious actions in the existing network.

We have taken 20 nodes and created networks in NS2 and obtained the result and observed the performance of algorithm initially. Later we have added an extra 180 nodes along with existing 20 nodes and obtained the result to test the scalability issue of an algorithm. DS -DPM algorithm is still performing well after scaled up the network and monitoring focus was also effective and the same represented in below diagram structure of DS-DPM system in Figure 1.

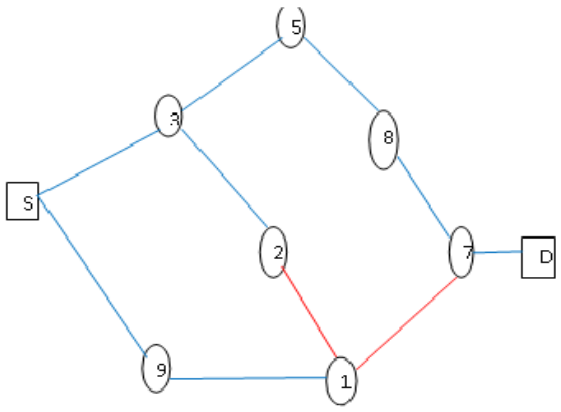


Figure 1:Structure of DS-DPM system

In the above Dynamic Scaled DPM is consists of S source, D-Destination and 1,2,3,5,8,9 are considered nodes between source and sink. Node 7 is considered an egress router and installed DS-DPM implementation which will monitor the flow of packet between the nodes. If any surge suspicious flow process happens which will identify and give warning to the specified nodes which are involve in surge flow transmission. Here S wants to transfer the data to D by passing packets between various located nodes. Blue lines were depicted in the above diagram are representing the normal flow of packet without any malicious action and on other hand Red lines are represented in the Figure 1 are attributed as malicious packet.

These nodes are called affected by zombies which will control these affected packets in the form of sending instructions.

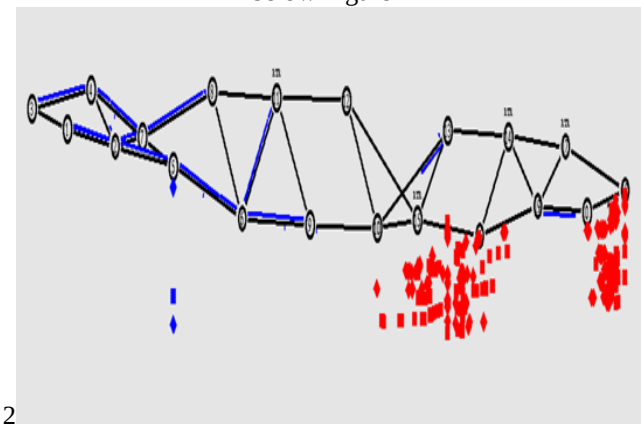
In the above represented diagram node 2 is harmed node because which never pass the packet to next hop to complete the transaction. Instead of forwarding packets which is started dropping packets in the network due to instruction given by the zombie. The regenerated path given by the DS-DPM algorithm is given below

Regenerated Path(RP) - { S-3-5-8-7-D }
Affected Path 1(AP1) - { S-3-2-1 }
Affected Path 1(AP1) - { S-9-11}

RP = SUGGESTION OF DS-DPM + LEGITIMATE NODES BETWEEN S and D

AP = IDENTIFICATION OF DS-DPM + ZOMBIES CONTROLL NODES

Both RP and AP is complete path will be generated with the involvement of DS-DPM algorithm after identification of victim. The same method is involved and implemented in our simulation result and we identified the node which are dropping packets instead of forwarding while transmission takes place in network. Simulation result of NS shown in below Figure



2

Figure 2 :Forwarding and dropped Packets

Nodes are created in NS2 and nodes are started transmitting packets. Blue lines and dots are normal flow of forwarding packets and red color dots are dropped packets due to malicious action.

DS-DPM Algorithm

Step 1 : Monitoring the Flow of Packets

[when n number of sources started their communication in the current infrastructure is being monitored in the aspect of forwarding packets in size]

Step 2 : Deviation of incoming flow from normal flow

[The measurement of packets flow is monitored of each station is need to compared with other node packet flow to find difference in the data flow.]

Step 3: Warning will be send to violating nodes

[Once the difference found in a specified station then a signal will be sent from coordinator to stop surge sending of packets]

Step 4: Node is marked in DS-DPM and timing monitored

[Proposed algorithm stores this violated node information immediately after warning]

Step 5:DS-DPM identify the malicious node which flood more traffic flow than normal

[Attack created node is identified through DS-DPM algorithm]

Step 6:Every AP is monitored by algorithm where AP is Actual Path between Source and Destination

[Path is estimated to send the data which no affected path]

Step 7:DS-DPM installed EGRESS router will generate the RP and same will be updated to Source

[Regenerated Path will be given to other nodes to transit the packet without any malicious action]

Step 8:The process will be continued even more nodes will be added up into the network.

[Finally algorithm is performing the same duty even after scaling up in the existing infrastructure]

The above 8 steps are actively implemented as code and the result is obtained in NS2 result.

Now explanation of ns 2 result of earlier implementation that is before scaled up output is explained.that is the Nam windowpane, just implements the moving picture (nam) statement, that's shaped even as disappearing for walks our simulation code. right here 7 nodes are created with node 0 unspecified as overhaul presenting nodule. other nodes are understood as supplier inquisitive for nodes. this is the comfort windowpane. Now, basically displays the node that's designated as a send-up node and Node arrangement parameters for configuring every one node. Node nothing is assigned as measuring node. It single-minded that node 4 is parody node.At precise time, the spoof node got monitored by means of the transporter generous node ‘zero’. And the packets,which is relocate beginning the node gets dropped through that supplier node. at the same time as executing Awkdrop.txt, the consequence might be strain out the information about the drops of each node sent. The higher than the be carried on the breeze version of every node in transmitting packets.Node`1,2,3,five,6 is transmitting less amount of packets at the same time as node 4 difference unbelievably deviated from the contradictory node inside the group of people.

Traffic corroboration module in planned mechanism must make sure the interchange availability surrounded by the network. ETS member of staff serving at table used to compute the rush forward slide along within the group of people. once the traffic reputation documented by means of ETS member of staff serving at table, it'll no longer launch further packets for communication. take for granted there may be no company justification router begins the marking system the tradition of DS-DPM method.

DS-DPM shops the transaction with of IP lecture to of all the packets forwarded passing through network. Dynamic array can be enhanced and abridged in keeping with the range of packet arrivals. the subsequent drawing long-established the filtering the every one distribution and in receipt of packets. The following result shows Figure 3 and Figure 4 node 4 is the suspected node because received packet is higher than other node

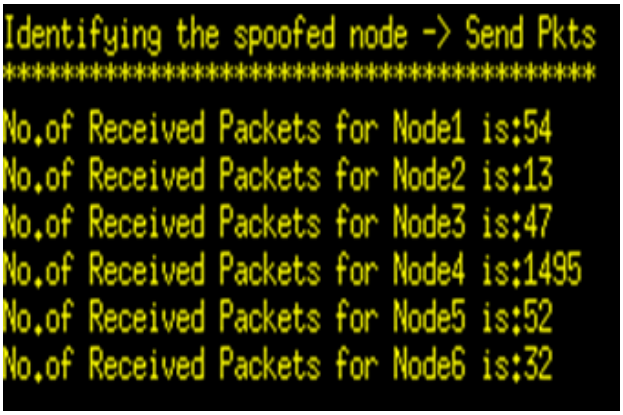


Figure 3:Identification of Spoofed node(Send packet)

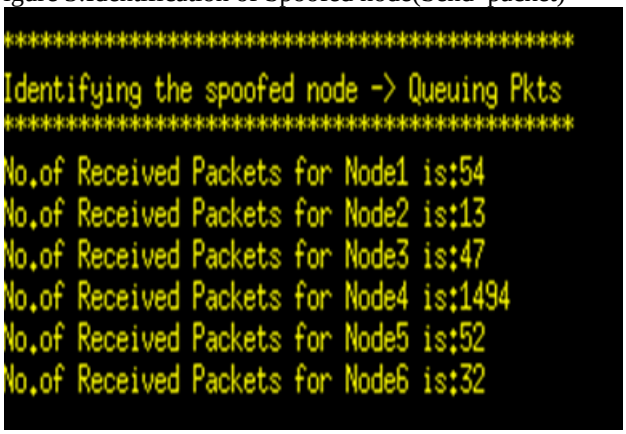


Figure 4: Identification of Spoofed node(Queuing packet)

Both above diagram shows clearly that the deviation between every node transmitting packets. Step 2 of DS-DPM algorithm demonstrates the deviation of actual delay with average delay .We compared to the previous DPM model with new model proposed in DS-DPM is given below Table 1.

Table 1 is containing information about the performance aspect of various algorithm by considering the different parameters of network behavior. Scaling is considered and we had given concentration only towards this to obtain different performance results.

Metrics considered	**Basic DPM**	**Flow DPM**	**Dynamic DPM**	DS-DPM
Scalable issues	Highly limited	slightly limited	No limited	Unlimited with good scaled up
Maximum traceable resources	Highly limited	slightly limited	No limited	Unlimited with good scaled up
Working Mode	Single	Single	Globally	Global with regeneration path
Storage	Heavy	Heavy	Light	Very Light
False positive	Inherent nature	Inherent nature	Non-Inherent in nature	Non-Inherent

Table 1 :Comparison of different DPM - Performance

IV.CONCLUSION

We have addressed many issues raised due to DDoS attacks in recent days application which are dedicatedly running under online server. We have given focus towards the performance of identification and detection process of victims to stop vulnerable activities in terms scaling up in the application. Our DS-DPM implementation meant to consider the scaled up network performance from current infrastructure. In the above table we have compared the various evaluation parameter in addition to that scalability. We obtained best result in scalability but very slight deviation observed in space storage management. There is a new proposal required in DPM techniques good in performance and improvement in storage and router overloaded performance.

REFERENCES

1. Vrizlynn L. L. Thing, *Student Member, IEEE*, Morris Sloman, *Member, IEEE*, and Naranker Dulay, *Member, IEEE* , "Locating Network Domain Entry and Exitpoint/path for DDoS Attack Traffic" IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 6, NO. 3, SEPTEMBER 2009 *page no163-173*
2. K. J. Houle and G. M. Weaver, "Trends in denial of service attack technology," CERT Coordination Center. [Online.] Available: http://www.cert.org/archive/pdf/DoS_trends.pdf, Tech. Rep., 2001 Oct. 2001.
3. Yang Xiang, Member, IEEE, Ke Li, and Wanlei Zhou, Senior Member, IEEE, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011 pp. 426–437.
4. G. Carl *et al.*, "Denial-of-service attack-detection techniques," *IEEE Internet Comput.*, vol. 10, no. 1, pp. 82–89, Jan./Feb. 2006.
5. P. Du and S. Abe, "IP packet size entropy-based scheme for detection of DoS/DDoS attacks," *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 5, pp.1274–1281, 2008.
6. S. Ledesma and D. Liu, "Synthesis of fractional Gaussian noise usinglinear approximation for generating self-similar network traffic,"*Comput. Commun. Rev.*, vol. 30, no. 2, pp. 4–17, 2000.
7. E. Perrin *et al.*, " th-order fractional Brownian motion and fractional Gaussian noises," *IEEE Trans. Signal Process.*, vol. 49, no. 5, pp.1049–1059, May 2001.
8. E. Perrin *et al.*, "Fast and exact synthesis for 1-D fractional Brownian motion and fractional Gaussian noises," *IEEE Signal Process. Lett.*, vol. 9, no. 11, pp. 382–384, Nov. 2002.
9. Y. Bao and H. Krim, "Renyi entropy based divergence measures for ICA," in *Proc. IEEE Workshop on Statistical Signal Processing*, 2003, pp. 565–568.
10. Qiao Yan and F. Richard Yu" Distributed Denial of Service Attacks in Software-Defined Networking with Cloud Computing" IEEE Communications Magazine • April 2015,pp 52-59
11. Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," IEEE Commun. Surveys & Tutorials, vol.15, no. 2, 2013, pp. 843–59. S. T. Zargar, J. Joshi, and D. Tipper, "A Survey of
12. Defense Mechanisms Against Distributed Denial of Service(DDoS) Flooding Attacks," IEEE Commun. Surveys & Tutorials, vol. 15, no. 4, 2013, pp. 2046–69.