Some Investigation on DDOS Attack Models in Mobile Networks

https://doi.org/10.3991/ijim.v13i10.11304

D.Yuvaraj (✉)
Cihan University, Duhok, Iraq
yuvaraj2626@outlook.com

M. Sivaram
Lebanese French University, Erbil, Iraq

A. Mohamed Uvaze Ahamed
Cihan University, Erbil, Iraq

S. Nageswari
Bhararh Niketan Engineeing College, Theni, India

Abstract—With advancements in device and communication technologies, there has been a great revolution in development of net gadgets and communication technologies like 4G, 5G etc., in parallel, there has also been a widespread increase in ways to illegally hack data available over the internet and tamper the services offered to the customer. Common attacks include spoofing, Phishing, fraudulent extraction of transaction information and customer details. There have been attacks to cause traffic congestion over the network by introducing artificial infection packets over the internet. Hence, there is a great necessity in research for defence mechanism against these attacks to ensure smooth and safe provision of services to customers. This paper investigates and elaborates the different types of attacks that may be incident on a system or a network, their features and attack mechanisms which provide useful insights into developing an attack resistant system. Almost all types of attacks have been discussed systematically in this research paper with special emphasis on distributed denial of service attacks.

Keywords—Network attacks, distributed denial of service attacks, flash crowds, and traffic congestion

1 Introduction

In recent times, there has been an increased threat in number of hacking incidents on a global basis. New kinds of threat are being introduced by hackers daily focused towards unauthorized access to hack data, tamper with given data, cause traffic congestion and thereby cause system hang which leads to the crash of entire network. This paper investigates the various basic concepts of these attacks with special emphasis on a specific type of attack namely the distributed denial of service attack (DDoS). The various research issues and challenges surrounding the implementation of an effective defence mechanism against these types of attacks have been elaborated and discussed in detail in this paper.

A denial of service attack poses serious menace to users denying services [11] through online networks causing a heavy congestion on the network. This is achieved by sending a large number of malicious packets from a single attacker system to the target system causing maximum depletion of system resources in terms of bandwidth and memory consequently leading to system hang and crash. A simple illustration of a denial of service attack is depicted in figure 3.1.

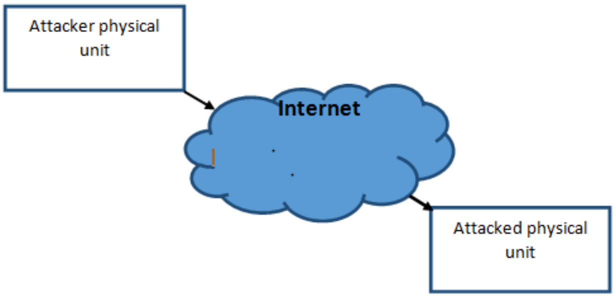

Fig. 1. Scheme of DoS attack on target

On the other hand, a distributed denial of attack [13] is more dangerous as it causes serious network bandwidth depletion and system crashes. It is more coordinated than DoS and multiple agents also known as zombies transmit the malicious packets of information to the target system.

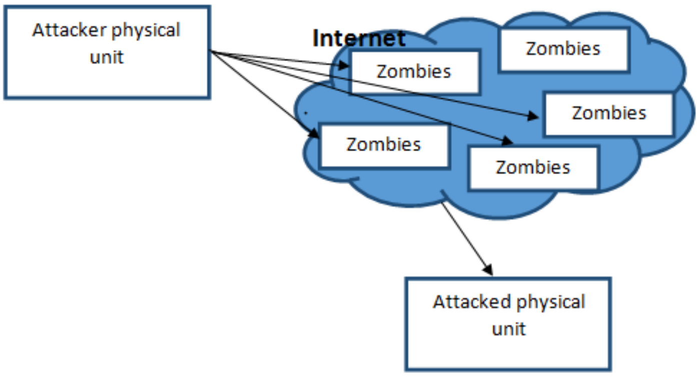

Fig. 2. Scheme of DDoS attack on target

These attacks are difficult to detect and much more consequential as multiple number of small sized packets of information are transmitted and the receiver or the attacked system receives them as an entire load of traffic and subsequently crash due to computational overload. A simple depiction of multiple zombies involved in a coordinated attack in DDoS is depicted in figure 2.

2 Ddos Attack Models

This section of this review paper presents an in-depth analysis into the various attack models and the various kinds of attacks that can be imminent on the system. Two categories of DDoS attack models [5] [8] [9] have been identified in the literature namely agent handler model and internet relay chat model also known as IRC. The two models have been depicted in structural organization form and discussed independently.

2.1 Agent based DDoS model

Figure 3 depicts the agent-based DDoS model where communication to other agents is achieved through handlers. The agents are predefined and specially configured nodes by the attacker to implement the instructions given to them by the attacker.

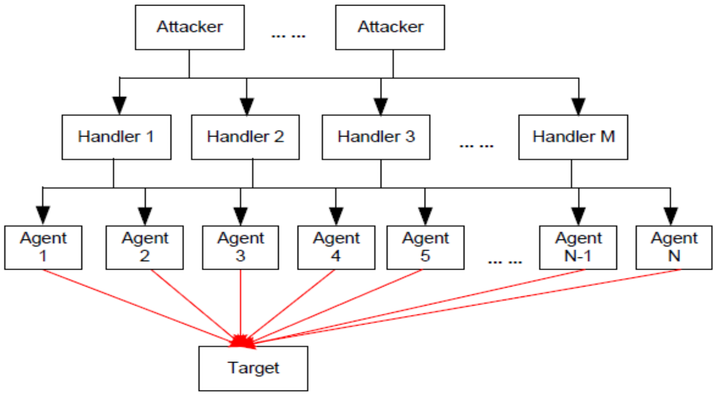

Fig. 3. Illustration of agent attacker model in DDoS

2.2 Internet relay chat DDoS model

The hierarchical operation of an internet relay chat model of DDoS attack on the target system is depicted in figure 4. It could be seen that relay chat network on the internet interconnects all the nodes in the environment to form a communication channel. The attacker then utilizes this communication channel to introduce their instructions to the agents which interact with the target.

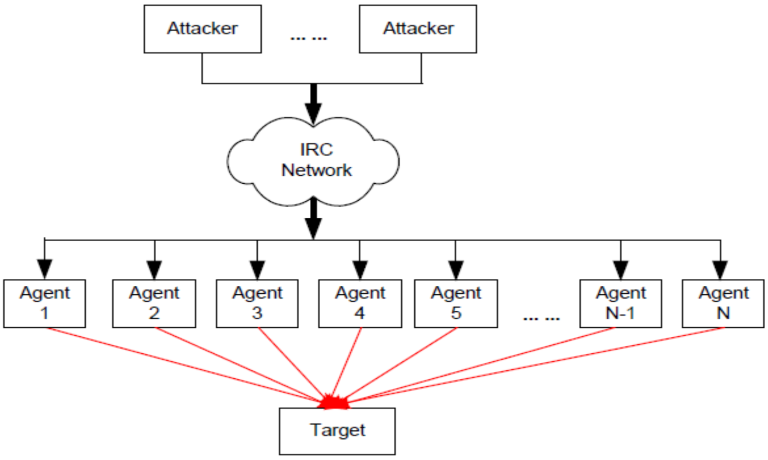

Fig. 4. Illustration IRC attacker model in DDoS

In both the configurations, the target systems are labelled the primary victims while the agents are termed as the secondary victims. In IRC based model [16], the attacker need not have the list of agents carrying out their instructions which eases the complexity and time of execution. The communication channels are established through IRC servers located around the environment under study. IRC is basically a multi connection internet chatting protocol. The DDoS attacks on target systems could be categorized into two major categories namely the Attack on resources class and Attack on route to resources class. A schematic illustration of the classification DDoS attacks based on the above mentioned two classes are depicted in figure 5.

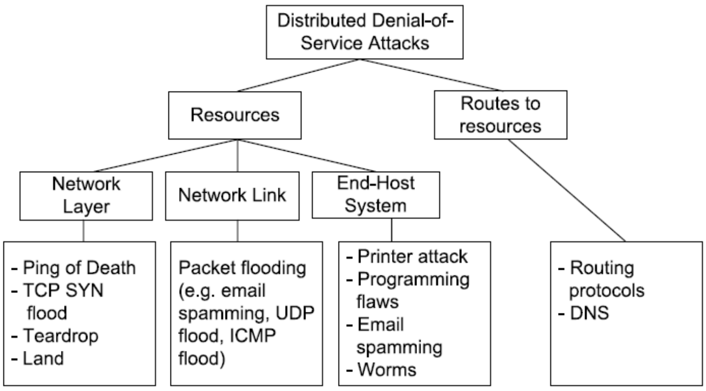

Fig. 5. Classification of DDoS attacks

2.3 Attack on resources

These attacks are engaged in a direct standoff with the resource of the target system and are further classified into three categories namely network layer attacks, network link attacks and end to host system attacks. In network layer attacks, the network layer protocols and links are attacked by the malicious infection while the network bandwidth is depleted in the network link layer attack. In the final class of attack, the main resources of the target system fall under the attack. These include the memory, clock cycle of processor etc., a wide range of attacks are listed under attack on resources category which have been elaborated in the succeeding sections.

2.4 POG (Ping of Death)

In POG attacks, the hacker transmits a packet of malicious data whose size is larger than the largest packet size of 64kB to the target system [11]. As a consequence, to this effect, the transmission unit is broken into smaller packets of illegal sizes and dimensions. On the contrary, the receiver will not be able to process the request until all these packets are received. This ultimately leads to congestion at the receiver point resulting in system hang, crash and reboots.

2.5 TCP SYN flood

It is a networking layer attack and motivation lies behind the handshaking process between server and client. A simple illustration of the handshaking protocol is depicted in figure 6.

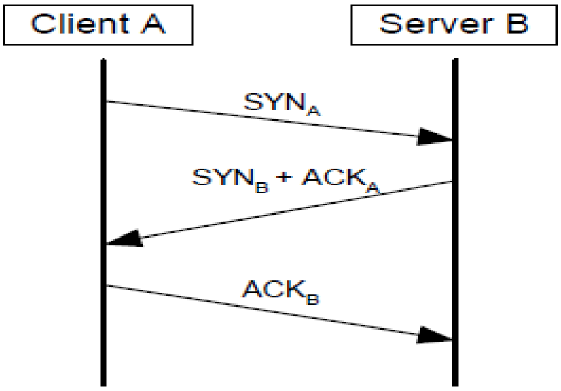

Fig. 6. TCP Handshake model

In the above figure it could be seen that when the server B receives the SYN packet, it responds back to server A with an ACK packet or acknowledgement packet. After the acknowledgement handshake signal, the communication between the two parties is established and required amount of CPU resources and memory are allocated for this communication process. Unlike the normal process as discussed above, during a TCP SYN attack, the hacker causes the agents in the network to issue fraudulent TCP SYN requests [10] to hold and bind the data and resources of the target system which denies the normal users to access the system resources to get their requests processed.

2.6 Teardrop

It is an attack towards the target system where the hacker through Tear drop sends fragments which exploit the concepts of IP fragment [3] [6] overlapping bug. This bug is unable to defragmented by the target system and hence consequently leading to system crash. These kinds of attacks were more prevalent in earlier versions of Windows like 95, 3.1, Linux 2.16 and older versions. However, patches are available to overcome these tear drop attacks. The recent versions of operating systems are quite resilient towards these tear drop attacks.

2.7 Land

Land is a specially custom-made attack targeting earlier versions like Windows 95, NT in which the source address and port are same as that of the destination an port addresses which consequently leads to system crash. Patches are available for this attack also but recent versions are quite resilient towards these kinds of attacks.

2.8 UDP flooding

This is a type of packet flooding where huge volumes of packets are transmitted from the attacker towards the victim. As a result of this huge volume of packets incident on the victim, the bandwidth gets saturated with these packets and legitimate users are denied access to get their requests processed.

2.9 Bombing

It is another variant of packet flooding class where email messages are sent to the victim in a repetitive manner and the contents of the email are scrap constructed out of garbage but consuming enormous size. This continuous bombardment with these illegitimate emails on the victim causes depletion of system bandwidth and resources denying access of services to legitimate clients.

2.10 Smurf

It is a form of bandwidth depletion attack and falls under the network link attack class. An ICMP echo packet is sent to the amplifier present in the network stream with a spoofed IP address directed towards the victim. This Echo packet is then broadcast to all other nodes within its coverage and each one in turn reflects back the ICMP packet directed towards the target system.

2.11 Fraggle

It is similar in operation to Smurfs but varies in sending an UDP echo which are transmitted to the character generation port in the system. The port reflects back this UDP echo directed to the IP address which is spoofed and aimed towards the victim. This initiates an infinite loop with each node reflecting this character echo towards the victim system in a continuous run.

2.12 Spamming

It is a slight variant of email bombing [17] and is concerned with transmitting large volumes of emails to all users consuming the victim's resources and time. There are also certain types of attacks which could be directed towards the system resources like printing, ink dispatch, wastage of papers etc.

2.13 Worms

They are a special class following an exponential distribution and are capable of self-propagation along the internet. A well-known worm in recent times is the code red which is found to penetrate and deplete the internet information server enabled machines. The self-propagating nature gives any user to reach a vulnerable web server in order to execute arbitrary codes on the system.

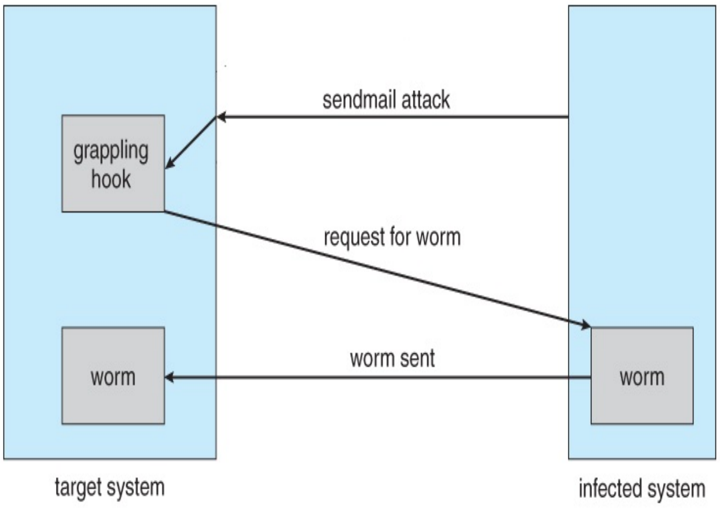

Fig. 7. Scheme of worm attack on target

Infected systems may experience web site defacement as well as performance degradation as a result of the propagating activity of this worm. In severe cases, the degradation will cause some services to stop entirely, since it is possible for a machine to be infected with multiple copies of the worm simultaneously.

2.14 Attacks on routes

As mentioned in previous sections, this is an indirect means of attack where the attacker targets the networks which serve as paths for traffic flow rather than engaging directly with the system itself. This is effectively countered by transmitting RIP [14] [15] packets into the network thus resisting a DDoS type of attack. RIP version 2 is an advancement of routing protocol to strengthen the network layer and prevent them from accepting protocols from unauthorized agents. A similar kind of protocol is the border gateway protocol which falls under the class of an inter-autonomous system routing protocol. BGP is effectively used to exchange routing information for the Internet and is the protocol used between Internet service providers (ISP).

3 Attack Responses

In this section, we discuss the DDoS attack response mechanisms classified into the following categories.

3.1 Traceback

A trace back is an effective attack response mechanism to reveal the identity of the attacker using a reverse propagation procedure. In general source and destination address are the two integral parts of an information packet.

A loophole existing in conventional packet delivery system is that the network does not verify the authenticity of the packet sender and none of the components in the networking path are responsible for the correctness of the address of the source. This weak procedure is exploited to a full extent by the DDoS hacker to conceal their identity with the help of spoofed IP addresses.

In order to respond to these kinds of attacks, trace backs have been used to trace the address of the original source and hold the sender accountable for the packet sent. Trace back at the source also helps in stopping the attack agent from propagating and infecting other nodes in the network. Two methods are practised in real time namely infrastructure scheme and end host scheme. An illustration of infrastructure scheme is depicted in figure 8.

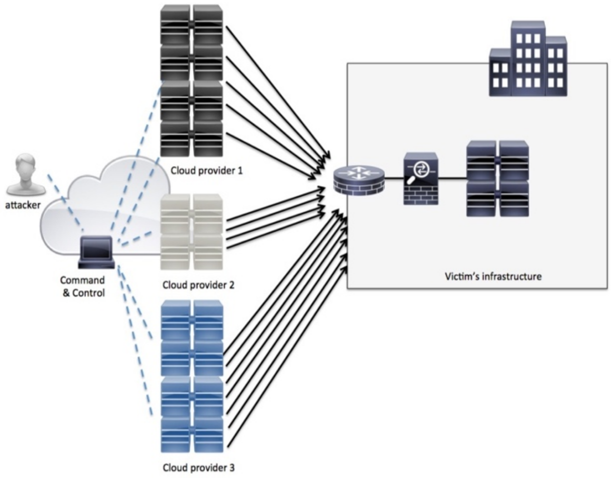

Fig. 8. Infrastructure based trace back scheme

As depicted above, the network is held accountable for storing and keeping track of the trace back data and to be utilizes as and when required to plot the attack pattern. An end host scheme is depicted in figure9.

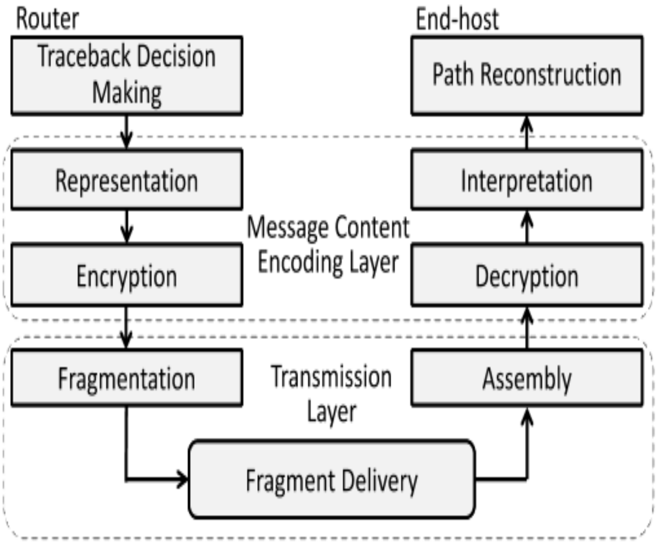

Fig. 9. Scheme of end host trace back approach

In the end-host scheme, the end hosts, which are the potential victims, maintain the traceback state information. IP marking and ICMP Traceback belong to this category.

3.2 Containment

The basic motivation behind containment of attacks is to control the intensity of attacks using dummy security systems in the special forms known as honey pots. They are characterized by limited security and their function is to entice an attacker to attack them and not the original network and systems. This process gives enough time and space for the defence mechanism to gain knowledge about the attacker, the attack type and pattern and to deploy and effective defence mechanism at the quickest time possible. The attackers in the form of DDoS attack the honey pots and, in the process, install their own malicious program code on the honey pot. This aids in the main system to study the program code and derive the attack pattern and their loopholes. These honey pots are further classified as low involvement, mid and high involvement based on their utility and features. Low honey pots have a passive approach towards defence mechanisms and may perform only eavesdropping. Mid-involvement Honey pots interact with the attacker to gain some knowledge but do not really expose the complete underlying operating system of main network to the attacker. High involvement honey pots are quite complex as they directly engage with the DDoS and emulate all services characteristic of the main system. They help capturing expansive information regarding the DDoS attack by exposing the real system to interact with the attacker in the virtual sense. They are complex and hence costly to implement in real time and also provide the risk of exposing any security vulnerabilities of the original system to the attacker.

3.3 Reconfiguration

In these types of attack response mechanisms, the configuration of the target system are manipulated so as to prevent the DDoS attacker to gain access of the legitimate path to the victim. An effective implementation of such a process is depicted in figure 10.

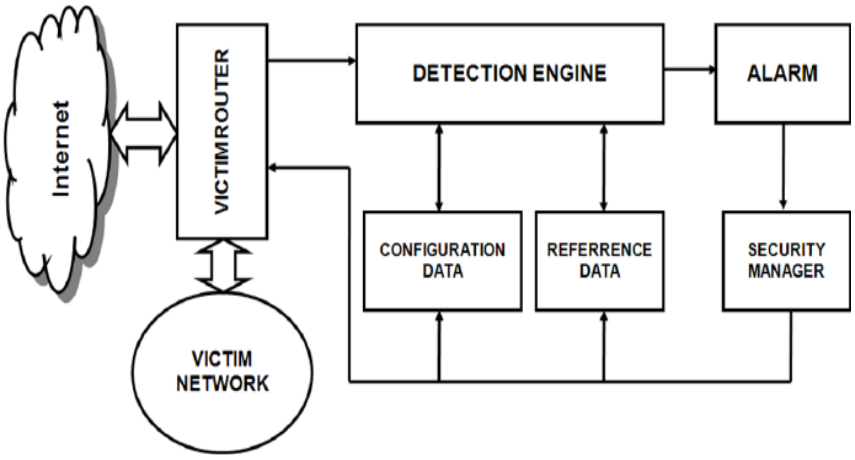

Fig. 10. Reconfiguration scheme of attack reaction mechanism

The architecture depicted in figure 11 is termed as secure overlay architecture in which the entry points labelled as overlay access points are responsible for allowing only valid and verified packets in the legitimate path to the victim network path. This architecture also provides an extra layer of security to the victim through high performance filters. Some algorithms utilized for implementing the reconfiguration architecture is the chord algorithm which is quite complex and relatively difficult to implement. Packets containing genuine source IP addresses are distinguished from those that contain spoofed addresses by redirecting a client to a new IP address and port number, through a standard HTTP redirect message.

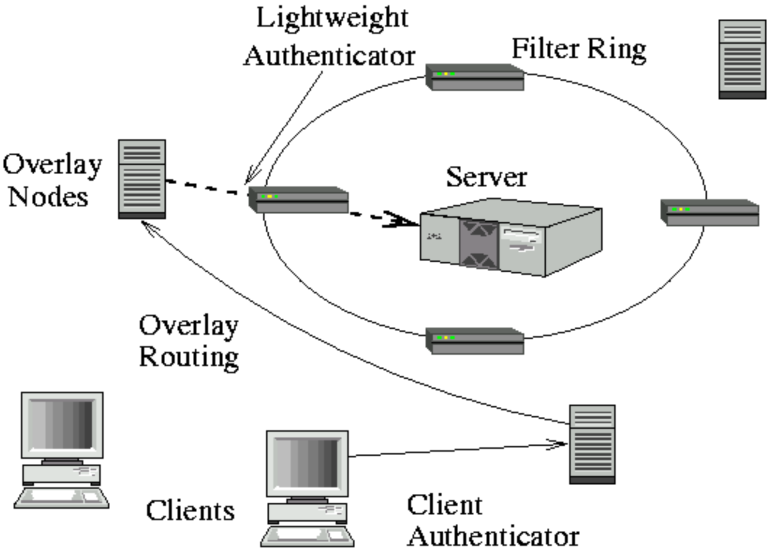

Fig. 11. Secure overlay architecture for reconfiguration

3.4 Redirection

In this scheme of attack response, the traffic is re-routed and prevented from reaching the target network. One such method is black hole filtering which allows an administrator to route the attack traffic to a null IP address and thereby drop it. On detection of an attack onset, a new route is created and the traffic attack with destination address of the victim is now redirected to the address of this new route with the black hole address where it is consequently dropped without any further propagation. Another variant of black hole routing is the sink-hole routing which follows the similar process but varies in the destination point by logging the attack traffic for further examination and analysis. Another notable process in redirection is shunting which operates within the network and the traffic is redirected to specific locations for analysis where they are differentiated from the malicious packets.

3.5 Filtering

These are the conventional mechanisms available for most of removal of DDoS attacks incident on the victim network. These function effectively only after sufficient analysis and inference that the suspected traffic is malicious in nature. This verification of malicious behavior is usually carried out by external tools or software. The detection is an essential stage before actually removing the malicious traffic. The detection may be anomaly based or misuse based. In anomaly-based detection schemes, a profile is created for every traffic pattern and the incident patterns whose extracted features do not match the created profile are designated to be malicious traffic. In some cases, a weakly defined detection scheme would detect traffic to be malicious if it does not match the profile but in reality, would not be an intrusion. They are classified to be false alarms and the amount of false alarms should be minimal for an effective filtering strategy. If detection is improper, it would consequently affect the filtering process and subsequently cause loss of data. On the other hand, misuse detection schemes employ signature patters which are quite efficient enough to detect variants of the same attack itself but however do not serve their full purpose in case of unknown attacks whose signatures are not stored in the profiles.

3.6 Rate limiting

As the name indicates, rate limiting cuts down the traffic flow volume to prevent the victim network being overburdened with overwhelming traffic. An effective rate limiting mechanism is the Pushback which is capable of imposing severe constraints on data stream which are detected and classified to be malicious. A drawback of this mechanism is that all traffic patterns irrespective of whether they are authentic or malicious suffer from the rate limiting constraint reducing the bandwidth and online speed for legitimate consumers.

3.7 Resource replication

Resource replication is a reaction mechanism initiated by the victim network and attempts to duplicate and multiply its resource availability to the DDoS attacker. The Xeno Service is a resource replication scheme to defend against DDoS attacks and is implemented as a distributed interconnection of hosts on the web by performing rapid replication and multiplication. By this process, the victim is able to gather more network resource in a short span of time and thus effectively absorb the effect of DDoS flood of packets thus continuing an uninterrupted quality service to legitimate users.

3.8 Legitimacy testing

In this mechanism, a legitimacy list is maintained and packets not listed in this array are classified into anomalous traffic. However, if a packet claims itself to be legitimate but still not on the list is subjected to a wide range of tests to prove its legitimacy. On inclusion of the suspected packet to the legitimacy list after successfully passing through a series of test, the normal transmission of data starts after established of communication link and control taken over by traffic management system. Net bouncer is one such effective mechanism which helps in differentiating legitimate traffic from illegitimate ones. Net bouncer also helps in differentiating DDoS congestion from flash crowd congestion situations. However, in spite of their efficiency in differentiation of authenticated traffic from malicious ones, they suffer drawbacks in terms of delay in processing as additional resources need to mobilised and allocated to carry out the legitimacy tests.

3.9 Resource consumption

An essential class of attacks is the connection depletion attacks carried out by DDoS attackers in which multiple requests for processing are initiated and left as such without solutions on the server input. This results in the server not being able to process requests from legitimate users due to rapid depletion of resources and memory utility. Client puzzle is one effective reaction mechanism which issues a number of small sized puzzles to all service requests initiators. Only legitimate users are able to solve the puzzle thus distinguishing themselves from illegitimate users. However, an effective filtering off anomalous traffic could be achieved through his method but at the cost of increased processing and computational cost.

3.10 Other mechanisms

Egress filtering is a well-known attack reaction mechanism and is basically dealing with filtering of outbound traffic from the network with the coefficients set to identify only valid packets of information. Spoofed IP address-based DDoS attacks could be effectively prevented by deploying a wide area connectivity of these filters. One such effective type of Egress filtering is D-WARD which controls the flow of outgoing traffic to the victim after malicious pattern detection.

Ingress filtering on the other hand is concerned with effective filtering of incoming or inbound traffic to the victim system over the network stream and packets with unauthenticated addresses are filtered out. It is simple in construction and easier to implement but still suffers from a widespread and coordinated from of DDoS attacks due to the wide range of spoofed IP addresses that the packets could take.

Another effective method for prevention of attacks is query based where queries are sent to the victim system where currently the attack is in progress and the response time of the query analysed and pattern studied to determine the type of attack imposed on the victim. On detection further flow of packets is stopped until the attack is contained.

4 Flash Crowds

Flash crowds are similar to DDoS attacks but are different in their intentions as they have no malicious intents. A flash crowd may be defined as sudden increase in traffic and access to particular website or network or online resource for a short period of time. An example could be thought of as a temporary website hosted for a short period of time which could be observed more in the case of sport-oriented tournaments or hosting of global events for a short duration of time. It is to be noted that the occurrences of these kinds of events could be known well in advance and sufficient preparations could be done to accommodate and manage such a huge volume of network traffic. Figure 3.12 depicts the flash crowd scenario in Atlanta at a particular point of time during the Olympics where servers and clients from several other places on a global place had to access the website of the Olympics experiencing a sudden surge in traffic for a significantly short period of time.

Figure 12 depicts the graphical plot of analysis of the surge in network traffic during flash crowd events. Another class of flash crowds is to anticipate an unexpected and unscheduled occurrence of flash crowds. The details regarding the pattern of distribution, the volume surge probability, duration of occurrence of flash crowd are completely made unaware to the base server.

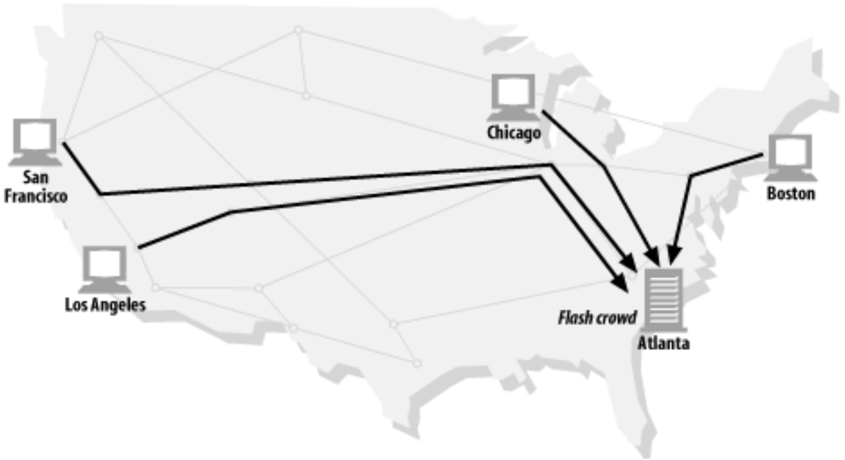

Fig. 12. Illustration of flash crowd scenario in Atlanta

Several approaches to effectively counter the flash crowd problem are found in the literature but at the cost of increasing cost of setting up the defence mechanism. The simplest method is to increase the volume of resources to effectively meet the unexpected demand on a trial and error basis. However, low demand on an unexpected schedule may incur heavy financial losses for gathering the resources.

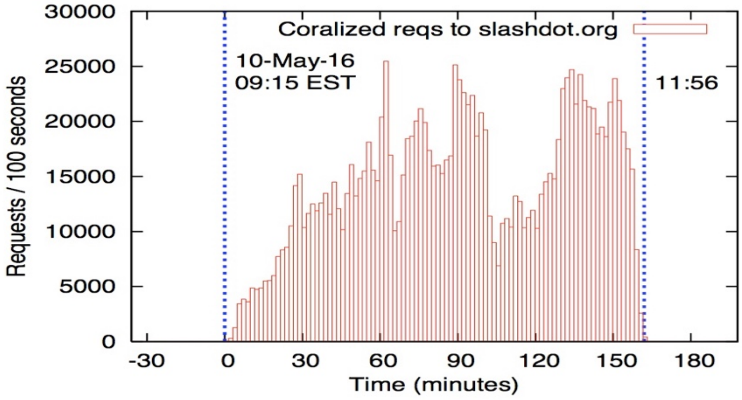

Fig. 13. Traffic volume distribution plot during flash crowd

Another approach is the content distribution network which aim to offload the workload from the main server to clusters of sub servers to effectively share and distribute the workload. Most of the webs hosting services utilize this CDN approach in spite of the fact that they are costly. Some of the nonprofit organizations however do not opt for this method and resort to conventional resources using the internet even though they are quite slow over the progress of flash crowd.

5 Conclusion

This paper has systematically and elaborately dealt with highlighting the methods of DDoS attacks on networks, their differing variants and the features of each one of them for designing and implementing an efficient defence mechanism. The different model of DDoS, their taxonomy with special emphasis on attack on resources and attack on routes to resources category has been presented in this chapter. The second part of the chapter deals with effective reaction mechanisms available to counter the attacks in real time. With these insights regarding the fundamental concepts and type of DDoS attack patterns and the various attributes defining them, a comparative evaluation strategy has been proposed in this thesis using three prominent techniques based on particle swarm optimization, artificial neural network and ant colony optimization. Each of these techniques have been exhaustively investigated and tested with practical observations visualized and tabulated to draw concluding remarks regarding the performance of these algorithms.

6 References

[1] Li G, He J, Fu Y (2008), "A group-based intrusion detection scheme in wireless sensor networks", In the 3rd international conference on grid and pervasive computing, pp 286–291. https://doi.org/10.1109/GPC.WORKSHOPS.2008.31

[2] Liao Y H, V. R. Vemuri (2002), "Use of K-nearest neighbour classifier for intrusion detection", Computers Security, Vol. 21, pp. 439–448. https://doi.org/10.1016/S0167-4048(02)00514-X

[3] Liu Y G, K. F. Chen, X. F. Liao, Wei Zhang (2004), "A Genetic clustering method for intrusion detection", Pattern Recognition, Vol. 37, pp.927–942. https://doi.org/10.1016/j.patcog.2003.09.011

[4] Lu, K., Wu, D., Fan, J., Todorovic, S., and Nucci, A. (2007), "Robust and efficient detection of DDoS attacks for large-scale internet", Computer Networks, Vol. 51, pp. 5036– 5056. https://doi.org/10.1016/j.comnet.2007.08.008

[5] Lu H, B. Zhao, X. Wang, and J. Su (2013), "Diff Sig: Resource differentiation-based malware behavioural concise signature generation", Information Communication Technology, Vol. 7804, pp. 271–284. https://doi.org/10.1007/978-3-642-36818-9_28

[6] Lu K, D. Wu, J. Fan, S. Todorovic, and A. Nucci (2007), "Robust and efficient detection of DDoS attacks for large-scale Internet", Computer Networks, Vol. 51, No. 1, pp. 9-22. https://doi.org/10.1016/j.comnet.2007.08.008

[7] Luigi HaoYue, LinkeGuo, Ruidong Li, Hitoshi Asaeda, Yuguang Fang (2014), "From data clouds: Enabling Community-Based Data-Centric Services Over the Internet of Things", IEEE Internet of Things Journal, Vol. 1, No. 5. https://doi.org/10.1109/JIOT.2014.2353629

[8] Manju Suresh and Neema M (2016), "Hardware implementation of Blowfish algorithm for the secure data transmission in Internet of things", Procedia technology, Vol. 25, pp. 248 – 255. https://doi.org/10.1016/j.protcy.2016.08.104

[9] Mohammad AL-Rousan, A. Rjoub and Ahmad Baset (2009), "A Low-Energy Security Algorithm for Exchanging Information in Wireless Sensor Networks", Journal of Information Assurance and Security, Vol. 4, pp.48-59.

[10] Mohammed A. Ambusaidi, Xiangjian He, Priyadarsi Nanda, Zhiyuan Tan (2016), "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm", IEEE Transactions on Computers, vol. 65, pp. 2986-2998. https://doi.org/10.1109/TC.2016.2519914

[11] Mostafa A. Salama, Heba F. Eid, Rabie A. Ramadan, Ashraf Darwish, and Aboul Ella Hassanien (2011), "Hybrid Intelligent Intrusion Detection Scheme", Soft Computing in Industrial Applications Advances in Intelligent and Soft Computing, Vol.96, pp.293-303. https://doi.org/10.1007/978-3-642-20505-7_26

[12] PrasantaGogoi, Monowar H Bhuyan, D K Bhattacharyya, and J K Kalita (2012), "Packet and Flow Based Network Intrusion Dataset", Contemporary Computing Communications in Computer and Information Science, Vol.306, pp.322-334. https://doi.org/10.1007/978-3-642-32129-0_34

[13] Perera C, A. Zaslavsky, P. Christen, and D. Georgakopoulos (2013), "Context aware computing for the Internet of Things: A survey," IEEE Communication Surveys, Vol. 16, No. 1, pp. 414-454. https://doi.org/10.1109/SURV.2013.042313.00197

[14] Perrig A, J. Stankovic, and D. Wagner (2004), "Security in wireless sensor networks," Communications on ACM, Special Issue: Wireless sensor networks, Vol. 47, pp. 53–57. https://doi.org/10.1145/990680.990707

[15] Phuong TV, Hung LX, Cho SJ, Lee YK, Lee S (2006), "An anomaly detection algorithm for detecting attacks in wireless sensor networks", In proceedings of Intelligent and security informatics, pp 735–736. https://doi.org/10.1007/11760146_111

[16] Pratap Chnadra Mandal (2012), "Superiority of Blowfish Algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9.

[17] Raj deep Bhanot, Rahul Hans (2015), "A Review and Comparative Analysis of Various Encryption Algorithms", International Journal of Security and its Applications, Vol. 9, No. 4. https://doi.org/10.14257/ijsia.2015.9.4.27

[18] Rajkumar and Manish Jitendra Nene (2013), “A survey on latest DoS attacks: Classification and defence mechanisms”, International journal of innovative research in computer and communication engineering, Vol. 1, No. 8, pp. 1847 – 1860.

[19] Raymond D. R. Midkiff. S. F (2008), “Denial of Service in Wireless Sensor Network: Attacks and Defenses”, IEEE Pervasive Computing, Vol. 7, Issue 1, pp. 74 – 81. https://doi.org/10.1109/MPRV.2008.6

7 Authors

Dr. D. Yuvaraj has completed his B. E (CSE) at J.J. College of Engineering and Technology, Bharathidasan University, Trichy, Tamilnadu, India. He received his M. Tech (CS&IT) degree from Manonmanium Sundaranar University, Tirunelveli, and Tamilnadu in 2004. He awarded PhD degree in Information and Communication Engineering (computer science and engineering) from Anna university, Chennai in 2017. He has nearly 19 years of experience in Teaching both UG and PG program. He is presently working as an Lecturer in Department of computer science, Cihan university – Duhok, Kurdistan Region, Iraq. His field of interest is in image processing, Data Mining, Image retrieval, Information retrieval and Artificial intelligence. He has published more than 30 papers in National journals and international journals. **Email id**: yuvaraj2626@outlook.com

Dr. M. Sivaram completed his B.E (CSE) at Bharat Niketan Engineering College, Madurai Kamaraj University, Madurai in 2002. He has awarded M. Tech (CSE) degree from National Institute of Technology, Trichy, and Tamilnadu in 2007. He Completed Ph.D. degree in Information and Communication Engineering from Anna University, Chennai in 2014. He has nearly 18 years of experience in Teaching both UG and PG program. He is presently working as an Assistant Professor in Department of Computer Networking, Labanese french University-Erbil, Kurdistan Region -Iraq. His field of interest are Data Mining, Information retrieval, Data fusion, Image Processing and Artificial intelligence. He has published more than 30 papers in International, National journals and conference.

Dr. Mohamed Uvaze Ahamed Ayoobkhan received his B.E and M.E degrees in Computer Science and Engineering from Anna University, Chennai, India. He has completed his PhD in Information Technology from Multimedia University, Malaysia. He worked as an Assistant Professor in the Department of Information Technology, Sri Ramakrishna Engineering College, Coimbatore India for the period of June 2012 to April 2014. He received a scholarship under Graduate Research Assistantship scheme from Multimedia University, Malaysia. Further he served as an Assistant Professor in Department of Computer Science and Engineering-Specialization, School of Engineering and Technology, Jain University, India from February 2018 to September 2018. Currently, he is working as an Assistant Professor, Cihan University-Erbil, Kurdistan region, Iraq. He has published 12 research papers in reputed international journals and conferences in the areas of Computer Vision and Machine Learning. Also, he is serving as a reviewer for international journals and conferences in the same field of research. His research mainly focused on Medical Imaging, Image compression/retrieval and Deep/Shallow Learning.

S. Nageswari completed her B.E (Electronics and Communication Engineering) at P.S.N.A College of Engineering and Technology, Dindigul, Madurai Kamaraj University, Madurai in 1998. She awarded M.E (Computer Science and engineering) degree at Jayaram College of Engineering & Technology, Trichy, Anna University of Technology, Trichy, and Tamilnadu in 2009. She has more than 15 years of experience in Teaching both UG and PG program and 1 years of Industrial experience. She is presently working as an Assistant Professor in Department of Computer science and Engineering in Bhararh Niketan Engineering, Theni. She has published more than 10 papers in International, National journals and conference

Article submitted 2019-07-07. Resubmitted 2019-07-30. Final acceptance 2019-07-30. Final version published as submitted by the authors.