Prevention, Detection and Mitigation of DDoS Attacks

Randall Lewis
MS Cybersecurity
DDoS or Distributed Denial-of-Service Attacks happens when an attacker sends a number of packets to a target machine. The attacker has accumulated a number of machines called “Zombies” under his control and from these machines is where the packet are sent from. TCP or UDP packets are sent out and this can flood a network/machine and cause it to freeze, shut down or crash. Preventing, Detecting and/or Mitigating this threat is the focus of my paper. I have chosen 3 research papers that discuss these methods.

The first research paper I am summarizing is the paper titled: “Detecting Distributed Denial-of-Service Attacks Using Kolmogorov Complexity Metrics” by A.B. Kulkarni, S.F. Bush, and S.C. Evans. This paper discusses the detection of DDoS (Distributed Denial-of-Service) that uses a concept called the Kolmogorov complexity. This theory states that the individual strings of an algorithm that are added up have a higher complexity that a group of random algorithmic strings (Kulkarni, 2002). This uses the traffic flow against the algorithm to detect the possibility of a DDoS attack. I chose this journal because it takes an unusual approach to detection of DDoS. They were thinking outside of the box in trying to determine the complexities which will indicate a DDoS attack.

The DDoS attack is detected using the theory that any 2 random strings of X and Y, K(X) and K(Y) are the complexities of the individual strings. But having K(XY) is the joint complexity of the concatenation of the string. This means that two strings multiplied together are more complex or equal to the sum of all the string multiplied together. This can be used to detect DDoS because it also assumes that the attacks have similar packets because they have the same destination address, execution pattern and so on. In this they have a pattern that is similar and the Kolmogorov Complexity can identify patterns and then detect if this is a DDoS or not.
The complexity differential is calculated as $K(x_1, x_2, \ldots)$ and if the packets are random then this will be equal to the complexity of the sum of all the individual packets. But if they have some different patterns then the complexity will be greater than a collected sample of the packets and will be sent to a Local Detector. This detector will evaluate the strings and determine what kind of attack it is.

The technique works by multiplying string that are random and then multiplying accumulated strings. The strings that are random will be greater or equal to the complexity to the strings that are multiplied together. The first multiplication is:

$$K(XY) \leq K(X) + K(Y) + c$$

$K(X)$ and $K(Y)$ are the complexities and $c$ is the constant.

The attack is determined by monitoring the complexity change in the algorithmic strings.

Then the complexity differential if computed: $[K(x_1) + K(x_2) + K(x_3) + \ldots + K(x_n)] - K(x_1x_2x_3\ldots x_n)$
In this \( K(x_1x_2x_3\ldots x_n) \) is the complexity of the packets concatenated together. If the packets are random then \( K(x..) \) will equal the sum of the individual complexities and the differential will then be 0. But if the number is greater than 0 then the packets will be deemed suspect and a sample is then sent to the local detector. After it is sent to the Local Detector then all the packets are sent to a Domain Detector and the attack is determined if it is local or distributed.

The proposed technique is not a promising practical approach to be implemented into an existing platform. For starters we can look in the research and see that they state that the technique needs to be compared to more intelligent detection algorithms that are in use (Kulkarni, A., 2002). There are databases of algorithms that are already in use and if the Kolmogorov Complexity technique is just reusing this information then it’s not practical. Also the entire packet has to be evaluated and before the decision can be made on the complexity of the packet. This evaluation will decrease processing speed and also use more space than allotted.

The Kolmogorov Complexity is also not computable but only methods to compute the estimates. In detecting DDoS attacks the technology has to be exact and not an estimate in order for false alarms to be minimized.

The strengths of this technique is that it takes a different approach to the detection of DDoS attacks in looking at the differences in the complexities. This is good because the attackers will mostly not try to hide their attack in this way. This detection technique also ends with trying to locate the source of the attacker. the Main problem with this attack is that the source is always spoofed which stops or slows down a response to fight this attack.

The weaknesses in this kind of attack are that the packets have to be completely inspected. This slows down processing time and in cases of a DDoS, slowing down will limit the functionality.
This technique also uses estimates and this will create a lot of false alarms. What will happen in time is that the false alarms will be quantified and documented by the database but other databases and techniques can be used to verify other known attacks. The other weakness is that this will show estimates of the complexity and not exact numbers.

The Second research paper is titled “Honeypot back-propagation for mitigating spoofing distributed Denial-of-Service attacks”. I will explore the mitigation method in this paper for DDoS attacks.

This paper uses Honeypot back-propagation which traces back to the source of the attack and stops it. Honeypots are effective in getting the attack signatures and Roaming Honeypots can hide the Honeypots in a pool of servers. This is done by activating and deactivating servers at certain sets of time and uses the other servers as Honeypots. The Roaming will make it hard for the attackers to identify active servers and then they will be lost in the Honeypot. What these two do together is that it is able to effectively trace back the attack and detect the signature. The reason why I chose this paper was because Honeypots are a very effective way to fight off an attacker.

This research uses Honeypots in an interesting and innovative way by changing servers from an active server to a Honeypot which will make getting into the network a lot more difficult. The paper describes the different types of DDoS defenses. In Spoofing prevention, IPsec is a way to prevent this. But the problem is that it can be used everywhere and the performance overhead is an issue. Also instances such as IP Spoofing with mobile technology legitimately use spoofing. Traceback is another defense and this can be use by using Packet marking schemes that can collect markings from the attacker on the router, but routers can be made vulnerable. There is also a mode called hop by hop traceback which traces the signature starting at the router next to
the router that was attacked. Mitigation is the other defense that is stated and this is done by avoiding a hash based routing, which can slow down the process 10 times, and taking action when the attack happens. But in the Roaming Honeypot defense the servers will then trigger a propagation of Honeypots when an attack stream triggers it. They will only activate during the attacks and in that will have a small overhead to deal with.

This Technique works by starting off with a Roaming Honeypot, this hides them within a pool of servers to start out with. In a pool of servers only certain ones will be active while the others are Honeypots then vice versa. This will make it hard for attackers to identify and divert their attention away from the Honeypot. The servers are changed on a certain schedule and the real clients will always send packets to a legitimate server. After the attack the source address of the attacker is then registered by the Honey pot and then blacklisted for any future attempts. When the servers go inactive it is switched to a Honeypot epoch and does not expect any legitimate traffic and if a packet is assigned to the inactive server then it is most likely an attack packet. At this point the signature of the packets is recorded.

This technique is a promising practical approach which can be effectively implemented. The goal for this technique is to capture the packets and then record the signatures to be able to trace back the host. When you use a Honeypot the attacker will be stuck inside of it and that is when the recording of the signature and address will take place. If the packets were just dropped then it would be harder to determine the source of the attack. Also in using the method of determining the attacks, the legitimate traffic will be able to get through and when legitimate traffic is stopped and inspected then a determination can be made that there was a false negative. The Roaming Honeypots is also a great technique because most attackers look for honey pots and they may notice them by their static positioning but when you have a roaming server that
goes from a “real” server to a Honeypot, an attacker can be easily fooled. This also keeps the servers from being compromised because of the consistent movement.

The strengths of this technique is that it is very versatile and not too common. Attackers will be more use to a static server in attacking and even to complete the attack they will have to redirect the packets when the servers are changed. and since the packets will all have one destination address for a DDoS attack, the Honeypot will get most of the packets and save the system.

The other strength is that the signatures will be recorded then put in a database and blacklisted. This stops future attacks and gives the victim the ability to know where the attack came from.

The Weaknesses in this is that it is complex and requires overhead. This process needs to be monitored and the database needs to be updated. The other weakness is a Honeypot in general. The servers are a way of letting the attackers in and they will be able to have some information about the network even if he is in the wrong place. Also if the attacker figures out the server schedule then the whole network can be compromised.

Preventing DDoS attacks is another option that we can look at. This would actually be an ideal solution to the problem of DDoS attacks if that was entirely possible. Mesh networks are a rising technology in which cities are being wired along with the wireless connection of site countrywide, this type of network needs to be protected and the need for this protection will only rise. This is the reason why I chose the next article because it is an approach that will continue because attacks and technology in this form have only scratched the surface.

The third research paper I chose is “An adaptive learning routing protocol for the prevention of distributed denial of service attacks in wireless mesh networks”. This will explore the option of preventing DDoS attacks and the technique in going about it. The way this paper goes about it
is to develop a new routing protocol called DLSR. This paper introduces LA (learning Automata) based components, proposes two new frame formats and a new algorithm to determine the route to the destination in the case of a DDoS attack.

The LA is a mathematical model that decides what actions to take based on previous actions. This uses the environment, a set of action and the system to make decisions. The DSLR will prevent a DDoS attack in 3 phases:

- DDoS detection.
- Attack identification
- DDoS defense mechanism

One of the frame formats is called The DALERT Packet (DDoS alert). This works by a DALERT packet being sent by the server when it thinks the network is under attack. This message will then alert all the Nodes and stop traffic from entering the network.

The technique behind this starts with the LA (learning Automata). This works with no knowledge of the networked environment making it random. It reacts based on the actions of the environment with input from knowledge of its previous actions. The system in turn become smarter. The Automaton uses a formula that is a bit complex using (Q,A,B,F, H) to represent different functions, i.e.:

Q is the state of the LA
A is a set of actions
B is the response from the environment
F and H are mapping functions.

These correlate with the environment in which are represented by (A,B,C)

A is the finite input
B is the output of the environment
C is a set of penalty Probabilities

This all put together can create a formula that will be confusing to the average man but will be able to make a decision based on the type of packets that come in and are deemed malicious.
The DLSR protocol works in three ways:
- DDoS detection
- Attack identification
- DDoS defense mechanism

The DDoS detection is done by analyzing the fixing a maximum amount of capacity for the server. When there is a higher number of request then the server has capacity, this is a DoS attack. When this happens the server goes into alert and sends the DALERT packet to the nodes to identify the attack. This packet sends out information in either 0(no threat) or 1(imminent threat). When this is done only the IP address is able to be identified and the identity of the attacker is the next step. All the packets will then get analyzed by sending a large number of server host.
request. When this happens the nodes then start dropping packets that are sent from the attacking server and analyzing other incoming packets.

This technique is an effective and practical approach that can be effectively implemented. Automata is already used in detecting a DDoS attack in other methods and this is just another method that uses a different kind of technique. LADS (large scale automated DDoS detection system) is an example (Sekar, V., 2006).

This also clearly states how the process is completed and how the nodes go from bringing packets in to then dropping packets. In the Experiment 3 of this paper the packet dropping behavior of the nodes were studied. (Sudip Misra, 2010). This study showed the number of server request sent by the attacker (X=258) and that a fraction of those were sent to the server (X< 25). This shows that the technique works because most of the packets are being dropped that are deemed malicious.

The strengths of this technique is that it covers the base and is basic enough to work and be effective. Detecting a DDoS is always the first step in preventing an attack. The technique is plainly laid out on how it is able to detect a DDoS attack and then take action on preventing one. using the LA technique is one of the other strengths also, Automation needs to used because of the amount of packets that come in.

The weaknesses of this method is that the sampling of all the incoming packets does take up energy and causes latency within the system which then slows down production. Also since there is a cost to sampling the packets, the researchers have proposed to use only certain nodes to sample and this will need another Automata system to decide on which actions to take.

DDoS attacks will only multiply and extend to other areas in the cyber world. Booz Allen Hamilton writer Jeff Lunglhofer writes “Obamacare kicks in over the next several years,
healthcare’s online presence is likely to explode” and “additional critical infrastructure sectors will be at risk. Online banking” (Lunglhofer, 2013). This shows that preventing, detecting and mitigating DDoS attacks is a thing of the present and will be a thing of the future and just as technology and Cyber crooks gets innovative, Cyber Security will have to be just as innovative.


