2016

Detecting Slow DDos Attacks on Mobile Devices

Brian Cusack
AUT University, brian.cusack@aut.ac.nz

Raymond Lutui
AUT University, raymond.lutui@aut.ac.nz

Reza Khaleghparast
AUT University, reza.khaleghparasta@aut.ac.nz

Detecting Slow DDos Attacks on Mobile Devices

Brian Cusack
Digital Forensic Research Laboratories
AUT University
Auckland, New Zealand
Email: brian.cusack@aut.ac.nz

Raymond Lutui
Digital Forensic Research Laboratories
AUT University
Auckland, New Zealand
Email: raymond.lutui@aut.ac.nz

Reza Khaleghparast
Digital Forensic Research Laboratories
AUT University
Auckland, New Zealand
Email: reza.khaleghparast@aut.ac.nz

Abstract

Denial of service attacks, distributed denial of service attacks and reflector attacks are well known and documented events. More recently these attacks have been directed at game stations and mobile communication devices as strategies for disrupting communication. In this paper we ask, How can slow DDos attacks be detected? The similarity metric is adopted and applied for potential application. A short review of previous literature on attacks and prevention methodologies is provided and strategies are discussed. An innovative attack detection method is introduced and the processes and procedures are summarized into an investigation process model. The advantages and benefits of applying the metric are demonstrated and the importance of trace back preparation discussed.

Keywords Slow DDoS, Detection, Mobile Devices, Metrics

1 Introduction

The lower bandwidth of mobile devices has prevented many of the more sophisticated attacks that are found on the Internet disrupting services. However, as the global proliferation of mobile device continues to expand with handsets and other communication devices, and attackers are finding ways to infiltrate. One of the more recent mobile phone attacks has been the slow DDOS attack that carefully obscures its tracks by fitting within the bandwidth on a time-based calculation. The attack slowly builds up momentum through compromised nodes and can become very costly for a user. These attacks create irritation for the end user by disrupting services but these disruptions and delays also create economic advantage for the service suppliers. The detection of these attacks requires new measures. In this paper we explore with dummy data from a mobile phone attack, the potential of the inter-similarity metric. The metric shows that it can quickly aggregate variations in log files over extended periods of time to identify patterns and consistencies that can disclose an attacker. The purpose of this is not only to alert the event but also to provide evidence in order to trace back to the attacker.

Cisco in Bailey et al. (2009) reported that smart devices were responsible for generating 14 times more traffic than a non-smart device. As a result, the cellular networks have made tremendous improvements in order to meet the demands for increased band with and QoS (Anstee et al., 2013). According to Farina et al. (2016), the 4G connections is responsible for generating six times more traffic than non 4G connections in 2015. However, globally, mobile data traffic reached 3.7 Exabyte per month in 2015; making mobile data traffic grow 4,000-fold over the past 10 years and almost 400-million-fold over the past 15 years. Smart devices represented 36 percent of mobile device connections globally in 2015. This accounted for 89 percent of mobile data traffic in which 55 percent was mobile video traffic. The average smartphone usage grew 43 percent in 2015. It is unambiguous in the literature that the cellular network will be the backbone that provides connectivity to a large amount of connected devices with various capabilities. It has ultra-high reliability but also a growing number of vulnerabilities (Chen & Song, 2005). Increasing demand from network users' for pervasive connectivity generates a demand for dynamic mobile networking. This also drives the growth in the development and usage of various mobile and wireless applications such as audio/video conferencing, distance learning, e-commerce, and distributed and multiparty games (Fernand et al., 2007). It has also led into an integration of various service infrastructures in order to provide all these services to users. As a result, cellular technologies will be the backbone to create connectivity to various devices and applications requirements. The wide variety of requirements carry new challenges to the cellular networks. Creating an architecture that can comprise performance, flexible functionality and security for the future connected industries is a challenge (Chen & Song, 2005). The characterization reveal by Network Science regarding the Cellular network and public switched telephone network: Relative Maturity is ranked High; Technology Intensity also ranked High; Societal Impacts/Benefits is ranked High and Societal Impact of Catastrophic Failure is ranked high as well (Deka et al., 2015).

For that reason, researchers in the field have been studying and developing various techniques to protect and prevent attacks on such network infrastructure (Arun et al., 2013). Real world systems can be represented by complex networks such as, social networks, communication networks, biological networks (Goodrich, 2008), (Gulisano et al., 2015), technological, transportation (Guo & Lee, 2010) and sociological (Guliisano et al., 2015). There structural complexity, and network evolution due to technological changes and connection diversity, are complex (Hendiks et al., 2014). A Complex network is defined as a large collection of interconnected nodes, where anything can be a node. For instance a person, an organization, a computer, a biological cell, and so forth. When Interconnected then two people know each other or two computers have a link connecting them for the purpose of passing information. These systems are considered complex because they are large and impossible to understand or predict their behavior. Due to the complex nature of these systems/networks, graph theory provides visualisation for the combination of switches and links that form a communication network (Hazeyama et al., 2003). This work focusses on assessing the vulnerabilities of the cellular communication network structure to a random or intentional attack; which can trigger the process of cascading failures. The criticality application of the similarity metric exploits the availability of log files and the relative spatial discrepancies between traffic expectations and abnormalities.

2 Previous Literature

Distributed Denial of Service (DDOS) is a type of Denial of Service (DOS) attack where an attacker infected a large number of systems with malicious software to gain control. The attacker then utilized those compromised systems to launch an attack on the targeted system (Robinson and Thomas, 2012, p.713). The purpose of DoS/DDoS is to flood the target system or service with a large number of requests.

This will eventually force it to shut down, in this manner, denying access to legitimate users (Chen and Song, 2005, p.526). Successful DDoS attack achieves two objectives, overpowering the victim's system and concealing the attacker's identity. Therefore, it is vital to monitor the characteristics of DDoS, as early detection of any variance to the system's normal activities can significantly increase the chance of preventing it and prioritizing them more accurately. The three components that researchers in the field are currently working on our detection, tracing back the origin of an attack, and preventing/defending (Robinson and Thomas, 2012, p.713).

The DDoS technique is very hard to detect and identify because it can be launched from hundreds or thousands of compromised nodes over the Internet. In this nature of attack, it also makes it hard to distinguish between legitimate network traffic and DDoS attack traffic. However, the vast variety of attacks in cyberspace indicate that the problem area is also vast and may very well be hard to conduct an exploratory study (Mirkovic and Reiher, 2004, p.39). DDoS has been further developed into a new type of DoS known as Low-rate DDoS. With this type of DDoS, attackers can now launch an attack using mobile SMART devices such as SMART phones. Last known report of this type of attack was reported by Murdock (2015) which involved 650,000 SMART phones. In the body of knowledge it is evident that there have been studies in this field trying to enhance the detection, mitigation and trace back mechanisms (Yu, 2014c, p.31). It is also evident that this type of cyber-attack is a major and continuous threat in cybersecurity (Yu, 2014b, p.1).

In the literature reviewed for this paper, it is evident that the main problem with DoS and DDoS attacks is the fact that, they are hard to detect, prevent/defend and trace back to the origin. The new generation of mobile communication has meant that we are now having mobile access to the wealth of information and services. Even though that its benefit is acknowledged but, a concerned is noted due to the proliferation of mobile technologies available (Serra and Venter, 2011, p.2). The advancement in the functionalities of technologies such as web-servers and cellular networks has enabled various applications to interact with each other. The advancement has also opened new opportunities in terms of security threats. For instance, attacks on mobile devices and cellular networks (Meyer and Penzhorn, 2004, p.20). Security researchers' stated that Smart devices now represent a particular risk. They function like computers, provide Internet connectivity from anywhere at any time and they can download applications or files, some could carry malicious code. Security experts are finding a growing number of viruses, worms and Trojan horses that target mobile devices. Security researchers argued that before long, hackers could infect mobile devices with malicious software (Leavitt, 2005, p.20).

Over the past decade, mobile devices have always been a victim of an attack such as data exfiltration as mobile devices contains large amount of probative information that can be linked to an individual (Kasiaras, et al., 2014, p.157). Today, processing and computational power of mobile devices is similar to that of a desktop computer and its potential to carry out offensive attacks on computer systems and services is certainly possible (Farina, et al., 2016, p.281). It is evident in the current literature that the usage of mobile devices is still increasing. As a result, they can constitute a target attack but are also an effective tool for launching distributed attacks such as a mobile botnet one (Farina, et al., 2014, p.385). Detection, prevention and trace back are the three main areas of DDoS that researchers are focusing on.

3 DOS/DDOS Topologies

There are different known network topologies for DoS/DDoS attack. However, the structure employed for a particular attack only depends on the attacker's preference.

A denial-of-service (DoS) attack is defined as an attempt to make a service such as a server or network unavailable to legitimate users by flooding it with attack packets. It's an attack on availability and there are four main DoS attack methods (Panko and Boyle, 2013, p.37).

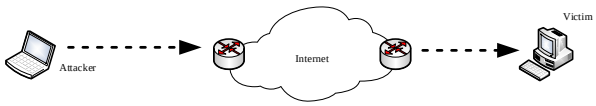

Figure 1: DoS topology (adopted from Panko and Boyle, 2013, p.37)

First is single source against single target (SSST) and second is and multiple sources against single target (MSST) (Xiuzhen, et al., 2011, p.221). The third method is named by Panko and Boyle (2013) as reflected and the fourth is sending malformed packets (p.198).

According to Yu (2014b), there two different types of DDoS attack structure – the typical DDoS attack and the Distributed Reflection Denial of Service (DRDoS) attack (p.3).

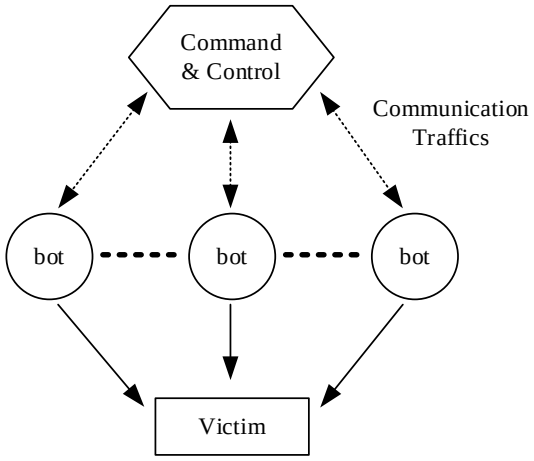

Figure 2: Typical DDoS topology (adopted from Yu, 2014b, p.4)

Figure 2 showed the network topology for a typical DDoS attack. In this environment, the attacker sends the command message to the command and control server to activate attack processes on all the bots (Yu, 2014b, p.5). The difference between the typical DDoS and the DRDoS is that, in DRDoS attack, the bot is control by the command and control centre.

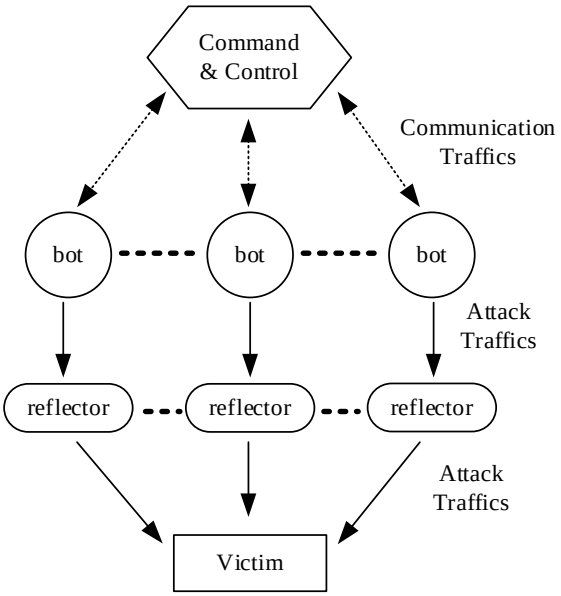

Figure 3: DRDoS topology (adopted from Yu, 2014b, p.5)

The bots send out stream of packets to the reflectors using the victim's IP address as the source address in the packet's header. As a result, the reflectors will flood the victim's system with respond traffics to what they believe a legitimate requests coming from the victim.

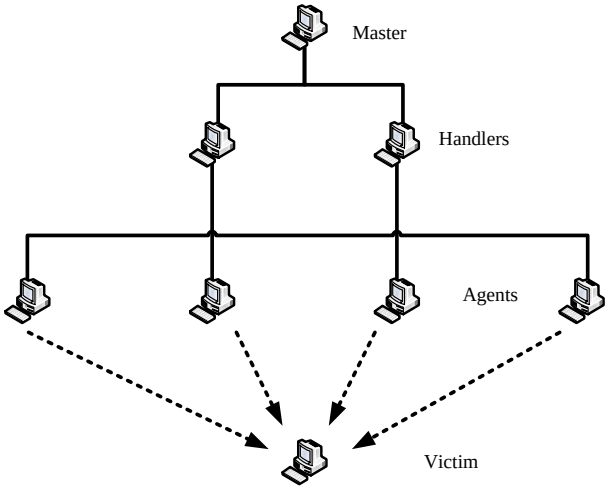

Figure 4: Constituents of DDoS (adopted from Deshmukh and Devadkar, 2015, p.204)

This architecture takes advantage of the client server technology. The Master forms the botnet by using the agents or bots and this known as the Zombies. The Master communicates with the Zombies via the Handlers. For instance, the Master sends out control commands to the Zombies via the Handlers (Singh, et al., 2016, p.112). Zombies are the nodes that are compromised by the Handlers, An attacker can compromise systems by scanning for vulnerabilities in the system. There are a number scanning techniques that an attacker can use such as Uniform scan worms, Hit list worm or the Routing worm (Zou, et al., 2006, p.702). Due to the rapid development in communication technologies, smart devices now can access the Internet via various wireless technologies such as Wi-FI, 3G, LTE or WiMax etc (Farina, et al., 2014, p.385). As a result, hackers can see the capabilities of engaging these devices in criminal activities. In the case of engaging these devices in a DDoS attack, specific malicious software such as worm or spyware is developed as means of creating a botnets to perform an attack (DDoS) attack (Stafford and Urbaczewski, 2004, p.297).

The network architecture in figure 5 showed that the attacker can use Wi-Fi network to create a botnet and launch an attack using the cellular network.

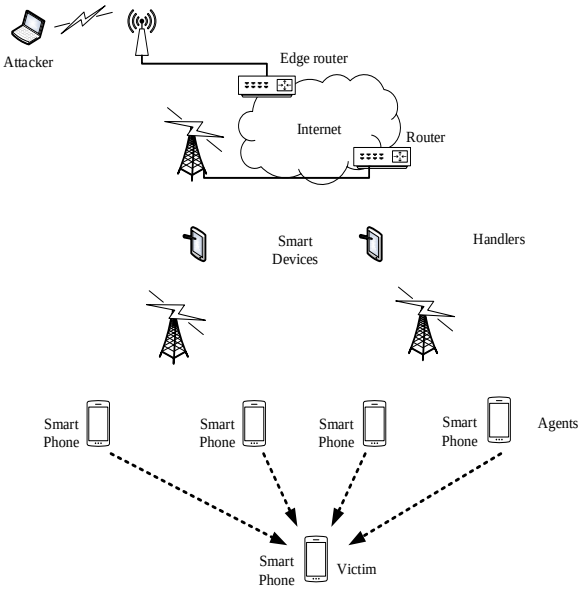

Figure 5: Mobile device DDoS topology (adopted from Hadiks, et al., 2014, p.507)

4 Proposed Method for Detection & Traceback

There have been known security incidents of DDoS involving Mobile devices. For instance, September 2015, researchers from CloudFlare reported that a DDoS attack peaked at over 275,000 HTTP requests per second and resulted in 4.5 billion hits on the targeted website. This was blamed on a malicious

advertising that compromised up to 650,000 Smartphones (Murdock, 2015, p.1). Various entities come together to create a cellular network and are grouped together based on their functions and interface requirements. As a result, these are divided into four main components: The Mobile Station (MS), The Base Station Subsystem (BSS), The Network and Switching Subsystem (NSS) and The Operation and Support Subsystem (OSS) (Androulidakis and Basios, 2008, p.465).

The vision of the 3G technologies is to use the IP technologies for control and transport. This cross network service collaborations will introduce a multi-vendor, multi-domain environment in order to gratify a wide variety of needs. This relationship will need to use Internet-based data and data from the cellular network in order to provide services to wireless users (Kotapati, et al., 2005, p.631). This new venture between these two different technologies introduces new vulnerabilities and exposes the users on the cellular network to a range of additional risks such as the DoS/DDoS attacks (Ricciato, et al., 2010, p.553).The introduction and growth of usages of technologies such as 4G/LTE and its high bandwidth has increased the pervasiveness nature of access points to the network. It is therefore evident mobile devices constitute not only a new target of an attack but its capability to execute an attack (Farina, et al., 2016, p.269). Contact list stored on mobile devices can be used to spread the malware and infect other devices (Plohmann, et al., 2011, p.133). A DoS/DDoS attack has evolved from flood to low bandwidth rate based also known as Slow DoS, Low-Rate DoS, Low Bandwidth Rate (LBR) DoS or application DoS. The purpose of this Slow DoS technique is to lower the amount of bandwidth and resources that are required to execute an attack. This new technique has been adopted and used in devices such as mobile phone (Cambiaso, et al., 2012, p.195). While most of the packets send to the target node in a flooding DoS attack may be useless but, in a low-rate attack, almost all of the packets play a role in the success of the attack. Therefore, the low-rate DoS will force the victim to process only the attack packets. There is not yet an effective taxonomy to address an efficient detection method in relation to slow-rate DoS (Cambiaso, et al., 2012, p.197). In this paper, the focus is on a technique to detect this kind of attack on mobile devices and also the use of digital forensics method to trace back the attack to its origin.

4.1 Distance Based Similarity Metric for Detection of Low-Rate DDoS Attack

Distributed Denial of Service (DDoS) is simple but a very powerful technique of attack (Douligeris and Mitrokotsa, 2004, p.643). The recent rapid development of mobile technologies has also led to a growth in their level of penetration. This growth also leads to a development of particular worms and other malicious software (Stafford and Urbaczewski, 2004, p.292). All these new advancements also led to a new type of DoS attack known as Low-rate DoS/DDoS attacks (Kuzmanovic and Knightly, 2003, p.75). Low-rate DDoS sends attack traffic periodically to the target device which is completely different from the traditional flooding DoS attack (Wu, et al., 2011, p.189). Various techniques for detection of the traditional flooding DDoS has been discussed in the literature. This section is designed to discuss and propose the use of the distance based similarity metric to detect a Low-rate DDoS attack. This metric has been used by Rasmi and Jantan (2013) and who propose a new algorithm known as Similarity of Attack Intentions (SAI) to estimate the similarity of cybercrime intentions for network forensics (p.542). Another study found that using self-similarity algorithm to detect DDoS can be difficult but it is possible (Brignoli, 2008, p.92).

Similarity has been used as the method for link predictions. For instance, x and y is assigned a score S_{xy} which can be defined as proximity or similarity between x and y (Lü and Zhou, 2011, p.153). The Similarity metric can be used in a more skilled approach such as using the node's attributes to define their similarity (Lin, 1998, p.298). Similarity has been used also to evaluate distances between nodes. The shorter the path between nodes, the more similar they are (Resnik, 1995, p.448). Distance based similarity metric is employed in this study to evaluate the similarity of the previous log file against the current log file in order to determine if a DDoS attack has occurred. Bajcsy and Kovačič (1989) argued that defining the problem will be the best way to fully understand the nature of the problem and what to match, i.e., what are the features to be used in matching; what are the constraints we have to consider; how to match, i.e., the matching process for achieving a consistent match; how to evaluate the match, i.e., define the similarity measure (p.3).

Protocols	**HTTP, HTTPS, ICMP, TCP, UDP, SYN, IRC**
Attributes	Time interval

Table 1. Characteristics of Low-rate DDoS.

To evaluate the similarity between two different objects *x* and *y*, a distance metric known as Euclidean Distance (*EU*) is used, which defines as follow:

$$EU\ (x, y) = \sqrt{(x - y)^2} \qquad (1)$$

This metric can also be generalized into n-dimensions points, such that a={x_1, x_2, ... x_n} and b={y_1, y_2, ..., y_n}. In this case, n-dimensions *EU* metric is defined as:

$$EU\ (a, b) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2}$$

$$= \sqrt{\sum_{i=1}^{n}(X_i - Y_i)^2} \qquad (2)$$

Let L_1 and L_2 be the existing log file and the current log file, respectively. Let x_i represent each protocol used in the existing log and y_i represent the protocol used in the current log, where $i=\{1, 2, ..., n\}$ and n is the total number of protocols as shown in table 1. In this case, L_1 ={x_1, x_2, ..., x_n} and L_2 ={y_1, y_2, ..., y_n}.

Euclidean distance can be normalized into a distance based similarity as follow:

$$S = \frac{1}{1+EU(L_1,L_2)} \qquad (3)$$

Similarity normalized *EU* into a value in between 0 and 1, where a value of 1 means that the two objects are identical and a value other than 1 means that the two objects are not identical.This study focuses on detecting the DDoS attack and identifying the means of the attack. Various protocols can be engaged in an attack such as it showed in table 1. In order to detect an attack, the similarity between the existing and the current log files are ranked. In doing so, the Euclidean distance between L_1 and L_2 is calculated first by using equation (1) and then the similarity can be ranked based on equation (3). Table 2, shows a simple case of calculating the distance based similarity of various protocols that were used in an attack. The sample data was taken from a live attack and then processed. Once the attack has been detected, the protocol that was engaged in the attack needs to be identified. When the detection processes are completed, a detailed report is developed for forensics. Table 2 illustrates the processes of distance based similarity.

Protocols	**HTTP**	**HTTPS**	**ICMP**	**TCP**	**UDP**	**SYN**	**IRC**
L_1	x_1=1000	x_2=800	x_3=600	x_4=2000	x_5=5000	x_6=6000	x_7=200
L_2	y_1=21000	y_2=1000	y_3=600	y_4=3000	y_5=7000	y_6=1000	y_7=500
$EU(L_1, L_2)$	***20000***	200	0	1000	2000	5000	300
S	***0.00005***	0.004	1	0.001	0.0005	0.0002	0.03

Table 2. A simple case of distance based similarity ranking.

4.2 Traceback Using Mobile Forensic Techniques

Mobile phone forensics is described as the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods (Curran, et al., 2010, p.1; Jansen and Ayers, 2007, p.4). Various digital forensics methods have been proposed by researchers around the world as a technique to trace back DDoS attackers. For instance, "attack pattern" is a technique that can be used to specify a generic way of performing an attack (Fernandez, et al., 2007, p.346). Guo and Lee (2010) proposed the use of Network forensics analysis method which relies wholly on the analysis of the IDS log files (p.294) Guo and Simon (2010) proposed an analytical model focusing on the analysis phase of network forensics procedure. This model will help forensic investigators in looking for patterns to determine if there is an anomaly in the traffic as result of an address spoofing flooding (ASF) attack. If there is an ASF attack, the model will also help to determine the time of when the attack was launched (p.135).

Kim and Kim (2011) proposed a Network Forensic Evidence Acquisition (NFEA) scheme with packet marking that offers an effective tracking scheme that can help network forensics investigators to trace back a DDoS attack to its origin. NFEA can guarantee the admissibility of the evidence acquired from the edge routers (p.392). Huang and Huang (2013) also adopted the network forensics method to investigate DDoS attack proposed Map (GHSOM) to look for variance in patterns of network traffic data (p.536). It is evident in the literature that there is yet much to understand with regards to the use of mobile forensics methods in the tracing back of DDoS attacks on mobile devices. The proposed trace

back method is based on the life cycle of the bot as shown in figure 7 (Silva, et al., 2013, p.381). The *Initial Infection* is the first phase where the device can be infected in several various ways. Provided that the first phase was successfully executed, the *second phase* is a secondary injection where the compromised device executes a program for malware binaries in a given network database (Silva, et al., 2013, p.384).

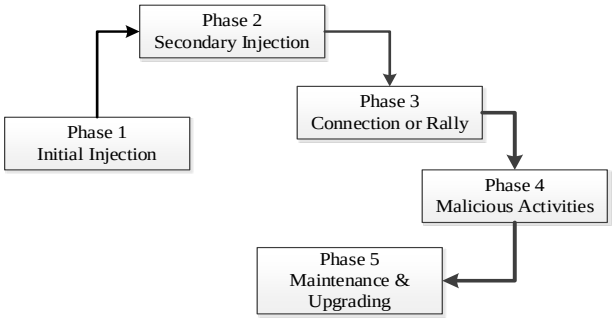

Figure 7: the Botnet's life cycle (adopted from Silva, et al., 2013, p.383)

The Malicious Activities phase allows the bots to communicate with the controller for instructions for conducting activities such as such as spam, DDoS and scanning. The final phase is the *Maintenance and Upgrade*. The bots continuously upgrades for various reasons such as, updating its codes to include avoids detection or to add new features (Zhu, Z., et al., 2008, p.967). Our proposed method is shown in figure 8, and the investigator methodology in figure 9. It is designed to take advantage of the botnet's life cycle and to use the attacker's own strategy against the attacker (Mulliner and Seifert, 2010, p.76). A malware will be placed in one or more of the bots in the botnet. When the attacker is returned to maintain and upgrade the bots, the malware can replicate itself to the attacker's device and it will reveal the attacker's location when the device is online (Polla, et al., 2013, p.448). Recently, hackers started attacking mobile devices with various strategies and malware such as Botnets, Backdoors, Rootkits and Trojans (Hsieh, et al., 2015, p.136). Symantec reported 2015 that in 2012, the main focus of mobile threat is information theft. 2013 was spying on users by tracking GPS coordinates and recording calls etc. 2014 the focus was on stealing device data and spying on the users (Symantec, 2015, p.22; Mell, et al., 2007, p.15). In terms of mobile devices, communication is the most important part of mobile botnet attack. Mobile devices have limited resources such as battery, network bandwidth, etc (Mulliner and Seifert, 2010, p.76).

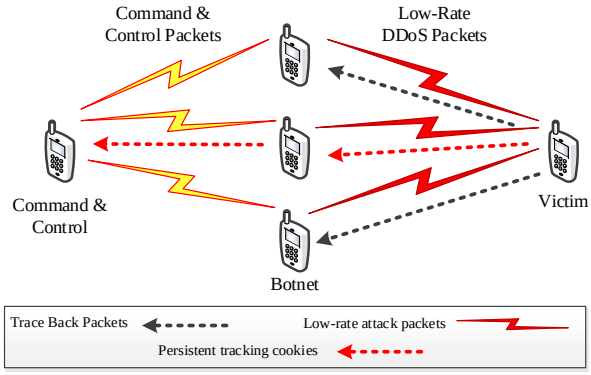

Figure 8 CtC trace back & investigation method.

Mobile forensics is defined as the science of recovering digital evidences from a mobile device under forensically sound conditions using accepted methods (Mumba and Venter, 2014, p.4). Mobile forensics investigation process consists of 15 phases however, it is divided into three main processes. The initialization process, the acquisition processes and the investigative processes. (Omeleze and Venter, 2013, p.5). The investigative processes consists of six processes. The Potential digital evidence acquisition, digital evidence examination and analysis, digital evidence interpretation, reporting, presentation and investigation closure (Mumba and Venter, 2014, p.4). The processes employed in this study only concern the examination and analysis phase as illustrated in figure 9. The results will be used by the CtC method to trace back the location of the attacker. These processes were designed not only to eliminate the irrelevant data but assure the admissibility of the evidence in the court of law. The mobile

forensics analysis process as illustrated in figure 9 starts with the data acquired from the victim's device. The data is used together with the reports from the similarity distance detection metric they can be calculated as a continuous process or on previous log data.

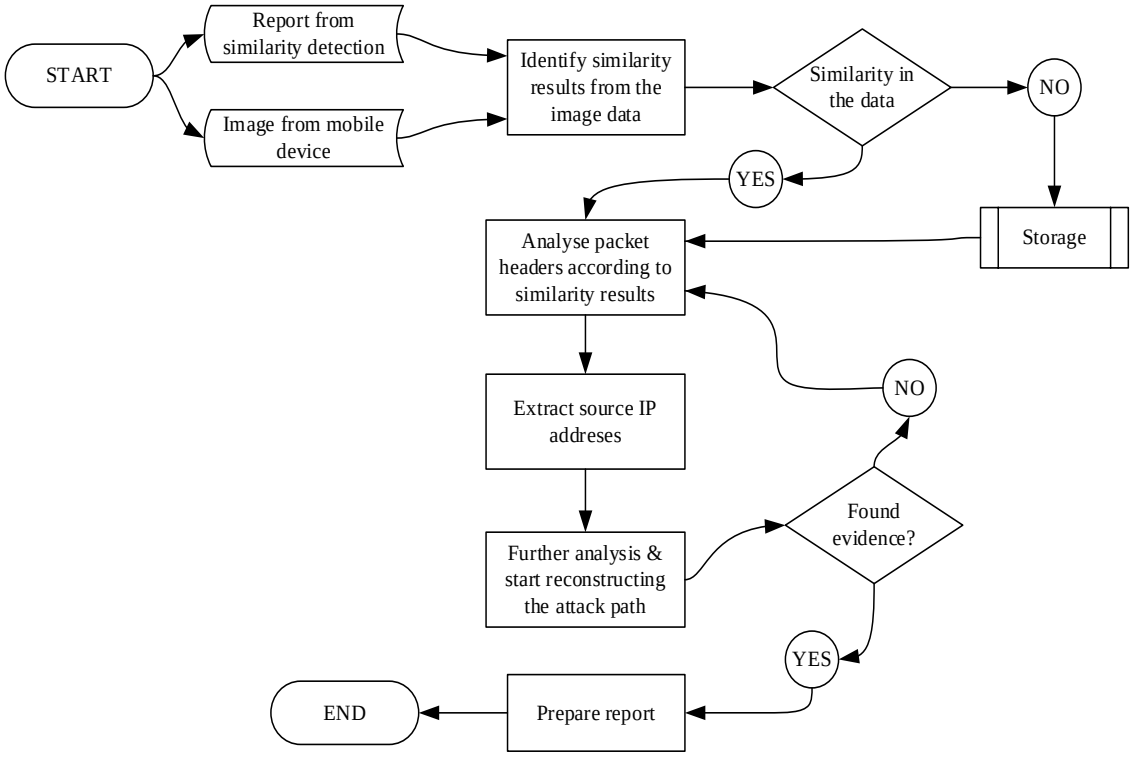

Figure 9: Mobile Low-rate DDoS forensics investigation process

5 Discussion

The foremost objective of mobile forensics method is to produce credible evidence of a crime committed that can be used to prosecute perpetrator. In this paper, the distance based similarity metric is applied to detect an attack from a slow DoS/DDoS onto a mobile device. The metric is also used to identify the nature of the attack for instance, which layer of the OSI model was the attack based on. The dummy data that we put through the metric to test the performance clearly showed when and where the slow DDOS attack occurred. Murdock (2015) reported that 650,000 SMART phones in China were compromised to launch an application layer DDoS attack. This attack generated 4.5 billion hits on the target (p.1). The detection feature of the metric as explained in section 4.1 will run a comparison of the current log against the benchmark log. When such an attack is detected then a closer look will be taken to identify the nature of the attack as illustrated in figure 7. Once the attack is confirmed and the nature of the attack is identified which in the above example is HTTP, a report is developed for forensics to start the investigation and the trace back process.

In the simple case shown in table 2, L1 shows the total requests from each protocol on the existing log. L2 shows the total requests from each protocol on the current log. EU(L1, L2) showed the results for each protocol when Euclidean distance is used to evaluate L1 and L2. S shows the results from EU(L1, L2) for each protocol after they have been normalized by similarity into a value in between 0 and 1. It is evident in the simple case showed and computed in table 2, that distance based similarity effectively improved the processes of detection, identification and investigation. This is due to the fact that the metric can identify the nature of the attack. Forensics will acquire the data, examine and analyze only the protocol(s) identified by the metric and start the attack path reconstruction process. Figure 9 is a unique contribution that is designed to facilitate investigation processes. The flow diagram optimises the use of information to guide a digital investigator through the use of the similarity metric. The processes also assure forensically sound actions are taken and in a logical sequence that can be reproduced and presented for a court of law.

The application and computation of the similarity metric demonstrates its applicability to slow DDOS attack detection. It provides an answer to the question of how can slow DDOS attacks be detected?; And also opens further research into the applicability of this metric in diverse situations and under different loadings. The potential is to automate the detection system based on live data and also for historical data. As such the metric has value for both security and forensic activity around mobile phones. The concept of disrupting mobile phone usage impacts the economic value and the social value of these devices. DDOS attacks provide economic value to the service providers because the owners of the mobile devices are locked into feepaying contracts of different descriptions. It is their phones and communication systems are exploited and they are liable for the costs. However, ebusinesses can be adversely affected when customers cannot get to their business opportunity or frustration levels reach a point where the customer's speak poorly of a particular service supplier. Similarly the disruption of emergency services and other critical resources can result. The detection and disruption of this type of attack is critical for the maintenance of confidence in mobile communication systems.

6 Conclusion

In this paper, distance based similarity metric is proposed as the method for detection and identification of slow DoS/DDoS attacks. The Euclidean distance metric was used to evaluate the similarity between the current and the benchmark logs. The distance based similarity metric was then used to normalize the evaluation results into a value in the range of 0 and 1. The result from the simple case developed to validate the method showed that the distance based similarity metric clearly detects and identify the attack and its nature. It is also evident in this study that the metric also effectively improved the performance, effectiveness and efficiency of the examination and analysis processes of the mobile forensics investigation. For future work, a general algorithm for detection and identification of such an attack under different conditions is being developed based on the distance based similarity metric. This will be used on a larger DDoS dataset to further evaluate the algorithm for accuracy and reliability.

7 References

Androulidakis, I., & Basios, C. (2008). A plain type of mobile attack: Compromise of user's privacy through a simple implementation method. Proceedings of the COMSWARE 3rd International Conference on the Communication Systems Software and Middleware (pp. 465-470). Bangalore: IEEE,

Anstee, D., Bowen, P., Chui, C. F., & Sockrider, G. (2016). Worldwide infrastructure security report. Special Repot: Arbor Networks, 11(1), 1-120.

Arun Raj Kumar, P., & Selvakumar, S. (2013). Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. Computer Communications, 36(3), 303-319.

Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009). A Survey of Botnet Technology and Defenses. Proceedings of the CATCH '09. Cybersecurity Applications & Technology Conference For Homeland Security (pp.299-304). Washington, DC: IEEE.

Cambiaso, E., Papaleo, G., & Aiello, M. (2012). Taxonomy of Slow DoS Attacks to Web Applications [Cambiaso2012]. In S. M. Thampi, A. Y. Zomaya, T. Strufe, J. M. Alcaraz Calero, & T. Thomas (Eds.). Proceedings of the International Conference, SNDS 2012 on Recent Trends in Computer Networks and Distributed Systems Security (pp. 195-204). Trivandrum: Springer.

Chen, S., & Song, Q. (2005). Perimeter-based defense against high bandwidth DDoS attacks. IEEE Transactions on Parallel and Distributed Systems, 16(6), 526-537.

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile Phone Forensic Analysis. International Journal of Digital Crime and Forensics, 2(2), 1-11.

Deka, R. K., Kalita, K. P., Bhattacharya, D. K., & Kalita, J. K. (2015). Network defense: Approaches, methods and techniques. Journal of Network and Computer Applications, 57, 71-84

Deshmukh, R. V., & Devadkar, K. K. (2015). Understanding DDoS Attack & its Effect in Cloud Environment. Procedia Computer Science, 49, 202-210.

Farina, P., Cambiaso, E., Papaleo, G., & Aiello, M. (2014). Mobile Botnets development: issues and solutions. International Journal of Future Computer and Communication, 3(6), 385-390.

Farina, P., Cambiaso, E., Papaleo, G., & Aiello, M. (2016). Are mobile botnets a possible threat? The case of SlowBot Net. Computers & Security, 58, 268-283.

Fernandez, E. B., VanHilst, M., Larrondo Petrie, M. M., & Huang, S. (2006). Defining Security Requirements Through Misuse Actions. In S. F. Ochoa & G.-C. Roman (Eds.), Advanced Software Engineering: Expanding the Frontiers of Software Technology, (pp. 123-137). Boston, MA: Springer.

Fernandez, E., Pelaez, J., & Larrondo-Petrie, M. (2007). Attack Patterns: A New Forensic and Design Tool. In P. Craiger & S. Shenoi (Eds.), Advances in Digital Forensics III: IFIP International Conference on Digital Forensics, National Centre for Forensic Science, (pp. 345-357). NY: Springer.

Goodrich, M. T. (2008). Probabilistic Packet Marking for Large-Scale IP Traceback. IEEE/ACM Transactions on Networking, 16(1), 15-24.

Gulisano, V., Callau-Zori, M., Fu, Z., Jiménez-Peris, R., Papatriantafilou, M., & Patiño-Martínez, M. (2015). STONE: A streaming DDoS defense framework. Expert Systems with Applications, 42(24), 9620-9633.

Guo, Y., & Lee, I. (2010). Forensic Analysis of DoS Attack Traffic in MANET. Proceedings of the 4th International Conference on the Network and System Security (NSS) (PP. 293-298). Melbourne: IEEE.

Guo, Y., & Simon, M. (2010). Network Forensics in MANET: Traffic Analysis of Source Spoofed DoS Attacks. Proceedings of the 4th International Conference on Network and System Security (NSS) (pp. 128-135). Melbourne: IEEE.

Hadiks, A., Chen, Y., Li, F., & Liu, B. (2014). A study of stealthy denial-of-service attacks in Wi-Fi direct device-to-device networks. Proceedings of the 2014 IEEE 11th Conference on the Consumer Communications and Networking Conference (CCNC) (pp. 507-508). Las Vegas, NV: IEEE.

Hazeyama, H., Masafumi, O., & Kadobayashi, Y. (2003). A layer-2 extension Oriented Computing and Applications (SOCA) (pp. 235-240). Matsue: IEEE.

Hsieh, W. C., Wu, C. C., & Kao, Y. W. (2015). A study of android malware detection technology evolution. Proceedings of the 2015 International Carnahan Conference on Security Technology (ICCST) (pp. 135-140). Taipei: IEEE.

Huang, S. Y., & Huang, Y. (2013). Network Forensic Analysis Using Growing Hierarchical SOM. Proceedings of the IEEE 13th International Conference on Data Mining Workshops (ICDMW) (pp. 536-543). Dallas: IEEE.

Jansen, W., & Ayers, R. (2007). Guidelines on Cell Phone Forensics: Recommendations of the National Institute of Standards and Technology. NIST: Special Publication 800-101, 1(1), 1-104.

Kasiaras, D., Zafeiropoulos, T., Clarke, N., & Kambourakis, G. (2014). Android forensics: Correlation analysis. Proceedings of the 9th International Conference on the Internet Technology and Secured Transactions (ICITST) (pp. 157-162). London: IEEE.

Kim, H. S., & Kim, H. K. (2011). Network Forensic Evidence Acquisition (NFEA) with Packet Marking. Proceedings of the Ninth IEEE International Conference on Parallel and Distributed Processing with Applications Workshops (ISPAW) (pp.388-393). Busan: IEEE.

Leavitt, N. (2005). Mobile phones: the next frontier for hackers? Computer, 38(4), 20-23.

Mell, P., Kent, K., & Nusbaum, J. (2007). Guide to Malware Incident Prevention and Handling: Recommendations of the National Institute of Standards and Technology. NIST: Special Publication 800-94, 1(1), 1-100.

Meyer, L., & Penzhorn, W. T. (2004). Denial of service and distributed denial of service-today and tomorrow. Proceedings of the 7th AFRICON Conference in Africa (pp. 959-964). Botswana: IEEE.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 34(2), 39-53.

Mulliner, C., & Seifert, J. P. (2010). Rise of the iBots: Owning a telco network. Proceedings of the 2010 5th International Conference on Malicious and Unwanted Software (MALWARE) (pp.71-80). Nancy, Lorraine: IEEE.

Mumba, E. R., & Venter, H. S. (2014). Mobile forensics using the harmonised digital forensic investigation process. Proceedings of the ISSA 2014 Conference on Information Security for South Africa (pp. 1-10). Johannesburg: IEEE.

Murdock, J. (2015). 650,000 Chinese smartphones used to launch ad network DDoS attack. Incisive Business Media, 1(1), 1-3.

Omeleze, S., & Venter, H. S. (2013). Testing the harmonised digital forensic investigation process model-using an Android mobile phone. Proceedings of the ISSA Conference on Information Security for South Africa, (pp.1-8). Johannesburg: IEEE.

Panko, R. R., & Boyle, R. J. (2013). Corporate Computer and Network Security (3 ed.). NY: Prentice Hall.

Plohmann, D., Gerhards-Padilla, E., & Leder, F. (2011). Botnets: Detection, Measurement, Disinfection & Defence. European Network and Information Security Agency (ENISA), 1(1), 1-153.

Polla, M. L., Martinelli, F., & Sgandurra, D. (2013). A Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials, 15(1), 446-471.

Ranjan, S., & Knightly, E. (2008). High performance distributed Denial-of-Service resilient web cluster architecture. Proceedings of the NOMS 2008. IEEE Conference on Network Operations and Management (pp. 1019-1024). Salvador, Bahia: IEEE.

Ricciato, F., Coluccia, A., & D'Alconzo, A. (2010). A review of DoS attack models for 3G cellular networks from a system-design perspective. Computer Communications, 33(5), 551-558.

Robinson, R. R. R., & Thomas, C. (2012). Evaluation of mitigation methods for distributed denial of service attacks. Proceedings of the 7th IEEE Conference on the Industrial Electronics and Applications (ICIEA) (pp. 713 - 718). Singapore: IEEE.

Serra, S. M., & Venter, H. S. (2011). Mobile cyber-bullying: A proposal for a pre-emptive approach to risk mitigation by employing digital forensic readiness. Proceedings of the 2011 Conference on the Information Security South Africa (ISSA) (pp.1-5). Johannesburg: IEEE.

Silva, S. S. C., Silva, R. M. P., Pinto, R. C. G., & Salles, R. M. (2013). Botnets: A survey. Computer Networks, 57(2), 378-403.

Stafford, T. F., & Urbaczewski, A. (2004). Spyware: The ghost in the machine. The Communications of the Association for Information Systems, 14(1), 291-306.

Symantec. (2015). 2015 Internet Security Threat Report. ISTR 20, 20(1), 1-119.

Wang, H., Jia, Q., Fleck, D., Powell, W., Li, F., & Stavrou, A. (2014). A moving target DDoS defense mechanism. Computer Communications, 46, 10-21.

Xiuzhen, C., Shenghong, L., Jin, M., & Jianhua, L. (2011). Quantitative threat assessment of denial of service attacks on service availability. Proceedings of the 2011 IEEE International Conference on Computer Science and Automation Engineering (CSAE) (pp.220-224). Shanghai: IEEE.

Yu, S. (2014a). Attack Source Traceback. In Distributed Denial of Service Attack and Defense (pp. 55-75). NY: Springer.

Yu, S. (2014b). An Overview of DDoS Attacks. In Distributed Denial of Service Attack and Defense (pp. 1-14). NY: Springer

Yu, S. (2014c). DDoS Attack Detection. In Distributed Denial of Service Attack and Defense (pp. 31-53). New York, NY: Springer

Zahid, M., Belmekki, A., & Mezrioui, A. (2012). A new architecture for detecting DDoS/brute forcing attack and destroying the botnet behind. Proceedings of the 2012 International Conference on Multimedia Computing and Systems (ICMCS) (pp. 899-903). Tangier: IEEE.

Zhu, Z., Lu, G., Chen, Y., Fu, Z. J., Roberts, P., & Han, K. (2008). Botnet Research Survey. Proceedings of the IEEE International Conference of the Computer Software and Applications (pp. 967-972).

Zou, C. C., Towsley, D., & Gong, W. (2006). On the performance of Internet worm scanning strategies. Performance Evaluation, 63(7), 700-723.