2016

Detecting and tracing slow attacks on mobile phone user service

Brian Cusack
Auckland University of Technology

Zhuang Tian
Auckland University of Technology

DOI: 10.4225/75/58a54b013185a
Cusack, B., & Tian, Z. (2016). Detecting and tracing slow attacks on mobile phone user service. In Valli, C. (Ed.). (2016). *The Proceedings of 14th Australian Digital Forensics Conference, 5-6 December 2016, Edith Cowan University, Perth, Australia*. (pp. 4-10).

DETECTING AND TRACING SLOW ATTACKS ON MOBILE PHONE USER SERVICE

Brian Cusack, Zhuang Tian
Digital Forensic Research Laboratories, AUT
brian.cusack@aut.ac.nz, zhuang_tian@hotmail.com

Abstract

The lower bandwidth of mobile devices has until recently filtered the range of attacks on the Internet. However, recent research shows that DOS and DDOS attacks, worms and viruses, and a whole range of social engineering attacks are impacting on broadband smartphone users. In our research we have developed a metric-based system to detect the traditional slow attacks that can be effective using limited resources, and then employed combinations of Internet trace back techniques to identify sources of attacks. Our research question asked: What defence mechanisms are effective? We critically evaluate the available literature to appraise the current state of the problem area and then propose an innovative solution for the detection and investigation of attacks.

Keywords: Slow Attacks, Detection, Trace back, Mobile, Communications

INTRODUCTION

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). An update (2016) notes that these attacks spike during the weekend, they are very large in size, and that these attacks are no longer targeted only at high profile websites but also at mobile services. 3G technologies use IP technologies for control and transport; and, require cross network service collaborations, multi-vendor, and a multi-domain environment in order to gratify a wide variety of needs. This relationship requires Internet-based data and data from the cellular network in order to provide services to wireless users (Kotapati, et al., 2005, p.631). 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 bandwidth and communication requirements (Anstee et al., 2013). According to Farina et al. (2014), the 4G connections are responsible for generating six times more traffic than non 4G connections. 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. Consequently our paper acknowledges the trends but addresses the traditional slow attack that works with all mobile devices of any bandwidth (Farina et al., 2016).

The new venture between the two different technologies introduces new vulnerabilities and exposes the users on the cellular network to a range of additional risks across the new surface (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 pervasive nature of access points to the network. It is therefore evident mobile devices constitute not only a new target of an attack but also it has the capability to execute an attack (Farina, et al., 2016, p.269). Contact lists stored on mobile devices can be used to spread malware and infect other devices (Plohmann, et al., 2011, p.133). A DoS/DDoS attack has evolved from flooding strategies to low bandwidth tactics that employ slow techniques and can operate in all bandwidths. The purpose of this Slow DoS techniques is to lower the amount of bandwidth and resources that are required to execute an attack. The slow techniques have been adopted and used against devices such as mobile phones and game stations (Cambiaso, et al., 2012, p.195). While most of the packets sent 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 tool to address an efficient detection method in relation to slow-rate DoS (p.197).

In this paper, we present an innovative technique to detect this kind of attack on mobile devices and also the use of multiple digital forensics methods to trace back the attack to its origin through the internet. The paper is designed to define slow attacks and to demonstrate our detection metric. We then present a flow diagram for investigation of slow attacks. The discussion on trace back reviews some of the previous and current literature in the field and draws the conclusion that two techniques working together are better than one on its own. We conclude by discussing

these claims and suggesting that slow attacks can be detected and managed to prevent loss of service to mobile phone users.

LOW RESOURCE ATTACKS

Low resource attacks rely on drip feeding malicious packets into a system. These techniques are often described as being slow because they are in contrast to flooding which rushes multiple packets through high bandwidth connections (Gilad and Herzberg, 2012). In contrast a low resource attack slowly drips malicious packets into a system such as a mobile phone where the victim processes every packet. Figure 1 shows the protocols which are open for exploitation by low resource slow attacks. The key element in each protocol is the ability for the attacker to slow down the attack packet by packet and to exploit the protocol mechanisms. Slow HTTP attacks, for example, rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an http request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

Table 1. Protocols for slow attack.

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

These types of attack are easy to execute because a single machine is able to establish thousands of connections to a server and generate thousands of unfinished HTTP requests in a very short period of time using minimal bandwidth. Due to implementation differences among various HTTP servers, two main attack vectors exist (Cambiaso, et al., 2012):

- **Slowloris**: Slowing down HTTP headers, making the server wait for the final CRLF, which indicates the end of the headers section; and,
- **Slow POST**: Slowing down the HTTP message body, making the server wait until all content arrives according to the Content-Length header; or until the final CRLF arrives, where if HTTP 1.1 is being used and no Content-Length was declared.

These attacks can just look like requests that are taking a long time, so it's hard to detect and prevent them by using traditional anti-DoS tools. In low resource conditions these attacks are effective because it does not require a large number of packets to create the effect. A defence against such an attack can be made by the following actions:

- Reject / drop connections with HTTP methods not supported by the URL.
- Limit the header and message body to a minimal reasonable length. Set tighter URL-specific limits as appropriate for every resource that accepts a message body.
- Set an absolute connection timeout nearing in mind that if the timeout is too short, you risk dropping legitimate slow connections; and if it's too long, you don't get any protection from attacks. A timeout value slightly greater than median lifetime of connections should satisfy most of the legitimate clients.
- The backlog of pending connections allows the server to hold connections it's not ready to accept, and this allows it to withstand a larger slow HTTP attack, as well as gives legitimate users a chance to be served under high load. However, a large backlog also prolongs the attack, since it backlogs all connection requests regardless of whether they're legitimate. If the server supports a backlog, make it reasonably large so your HTTP server can handle a small attack.
- Define the minimum incoming data rate, and drop connections that are slower than that rate. Care must be taken not to set the minimum too low, or you risk dropping legitimate connections.

However, these actions provide some protection but they do not signal a slow attack is taking place – which we address by innovation in the next section.

DETECTING ATTACKS

Distributed Denial of Service (DDoS) is simple but a very powerful technique of attack that disrupts service (Hadiks et al., 2014). The recent rapid proliferation and development of mobile technologies has also led to the exploitation for service disruption (Stafford and Urbaczewski, 2004, p.292). New techniques have also been developed to exploit the capacities and the characteristics of the service. This is where the DoS attack known as Low-rate DoS/DDoS attacks has evolved (Wang et al., 2007). Low-rate DDoS sends attack traffic periodically to the target device which makes it hard to detect amongst the normal traffic (Cambiaso et al., 2012). Various techniques for detection of the traditional flooding DDoS has been discussed in the literature. This section is designed to define and propose the

use of the distance based similarity metric to detect a Low-rate DDoS attack. The metric has been used in other contexts by Riccardio et al. (2010) who proposed a Similarity of Attack Intentions (SAI) to estimate the similarity of cybercrime intentions for network forensics. Another study found that using self-similarity algorithm to detect flooding DDoS attacks (Yu, 2014b). It has been used as the method for link predictions that compare one data set with another. For instance, *x* and *y* is assigned a score S_{xy} which can be defined as proximity or similarity between *x* and *y* (Yu, 2014a). The Similarity metric can be used in a more skilled approach such as using node attributes to define their similarity (Yu, 2014c). Similarity has been used also to evaluate distances between nodes. The shorter the path between nodes, the more similar they are (Snoeren et al., 2012). 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. Hadicks et al. (2014) 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). The challenge in slow or low-rate DoS/DDoS attack is to map the proximity between attacking packets for identification, and then to initiate trace back methods based on the identified packets.

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

$$EU\ (a,b) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2} = \sqrt{\sum_{i=1}^{n}(X_i - Y_i)^2}$$

To apply this metric to a Web server or to a mobile device then the log files have to be isolated for analysis. 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 where, L_1 ={x_1, x_2, …, x_n} and L_2 ={y_1, y_2, …, y_n}. For computational purposes the Euclidean distance can be normalized into a distance based similarity as follow: $S = \frac{1}{1+EU(L_1,L_2)}$

The normalized *EU* delivers 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. Consequently the analysis focuses upon the discrimination between two known log files. The differential will indicate changes that can inform the alert of an attack. For the DDoS attack various protocols can be engaged in an attack (see figure 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 by using the first equation and then the similarity can be ranked based on the second equation. Table 1 provides a worked example of the detection metrics being applied to a sample set of mobile attack data that was downloaded from the Internet to illustrate the use of the detection system. It is a simple case of calculating the distance based similarity of various protocols that were used in the 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

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

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

attack needs to be identified. This data in Table 2 shows in the S row that only one ICMP sample was the same. The variations in the other protocols indicates that an attack is occurring through them.

INVESTIGATING SLOW ATTACKS

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 consist of 15 phases that are 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. The results will be used to determine a slow attack first and then initiate trace back the potential location of the attacker (Curran, et al., 2010; Omeleze et al., 2013). These processes were designed not only to eliminate the irrelevant data but assure the admissibility of the evidence in the court of law (Jansen, et al., 2007). The mobile forensics analysis process as illustrated in figure 1 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 live process or from previous log data.

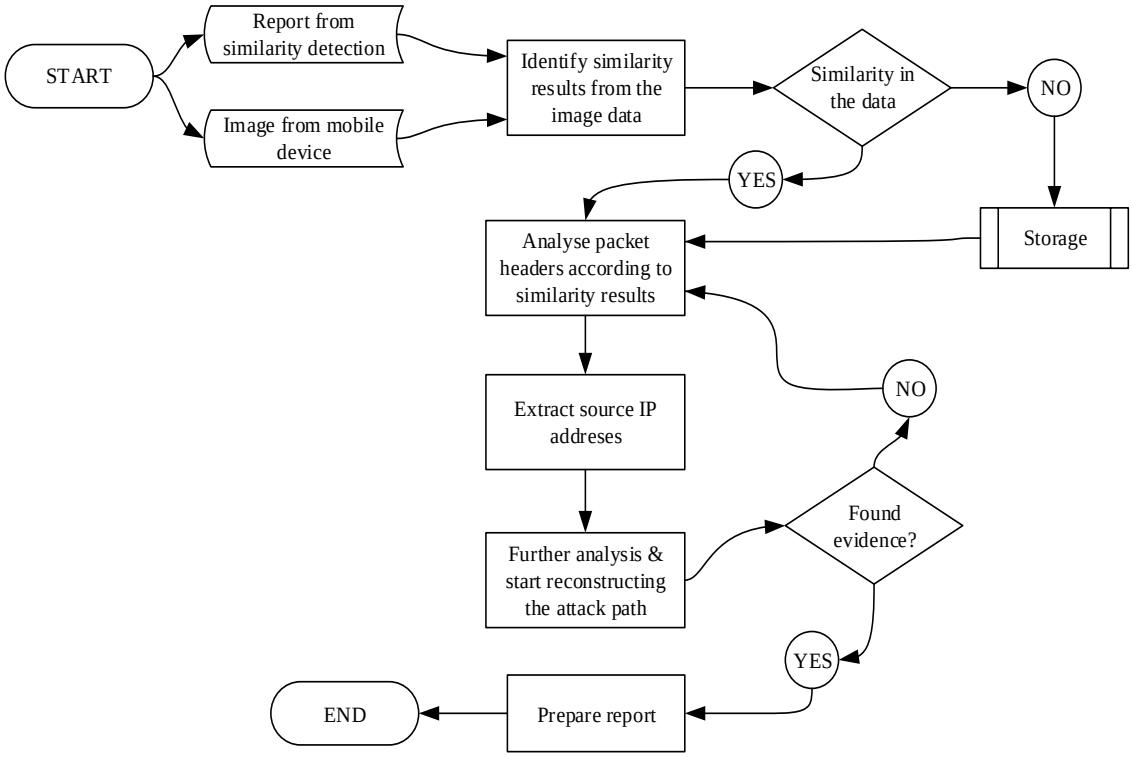

Figure 1. Mobile Low-rate DDoS forensics investigation process

Figure 1 assumes the common forensic soundness criteria are applied to correlate practice management by answering the questions: What meaning can be extracted from the evidence? What are the potential error factors? What are the training requirements for forensic practitioners? The model was developed to systematise processes while we investigated a number of slow attacks.

TRACEBACK

Traditional trace back methods are well-established for the Internet and broadband devices. The evidence presented in the introduction to this paper suggests that the majority of mobile phones are not broadband but the broadband phones produced most of the traffic. In addition all phones have some form of connectivity to the Internet. Therefore it is our argument that we can evaluate the traditional trace back methods and select the ones that are most appropriate for tracing back slow attacks. One reason that spoofing is often facilitated in these and other DoS or DDoS attacks is that it allows evasion of filters and quotas based on sender IP address, making tracing attackers harder (Devasundaram et al., 2006). Yu (2014b) reinforces that tracking back to the attack origin in DDoS attacks is a difficult and non-trivial problem due to the following reasons. Firstly, it is easy to forge or modify IP address (e.g. IP spoofing). Secondly, the stateless nature of IP routing, where routers normally know only the next hop for forwarding a packet instead of the entire end to end path taken by each packet, makes IP traceback even harder. Moreover, the Internet was originally designed for fast file sharing in a trusted environment and the network security was less important than communications, as it was a secondary consideration. Routers do not verify the source address of IP packets and the entire routing table is constructed on a trust basis. However, there are methodologies they can trace back to the last router from single packets. These methods can also be applied to trace back slow attacks, packet by packet (Goodrich, 2008).

A number of trace back methodologies can be rejected because they are impractical or too costly to implement. With slow attacks we are dealing with single packets or periodic clustered dispersions which are drip fed into a system to compromise devices. The metric can detect these time based malicious packets and once an alert sounded, trace back methods can be employed. A slow Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using some specific network utilities such as a website, web service or computer system (Hadiks et al., 2014). It is also a coordinated attack on the availability of the service of a given target system or network. It can be launched indirectly through many compromised computing systems. The websites or other mobile devices used to launch the attack are often called the 'secondary victims' (Izaddoost et al., 2007). The use of secondary victims in a slow DDoS attack provides an attacker with the ability to launch a much larger and more disruptive attack than a slow DoS attack while remaining anonymous since the secondary victims actually complete the attack, and hence make it more difficult for the digital forensic investigator (DFI) to track down the original attacker. In general, there are two types of standard attacks (Leavitt, 2005): direct and reflector attacks. In a direct attack, an attacker sends attack packets directly towards the victims. Attack packets can be any of the protocols in figure 1. (Kumar et al., 2011). In each attack on a mobile device a variety of networks are being used. The first instance it may be a Wi-Fi connection, or a direct cellular signal, or any other wireless protocol. Although it may be theoretically possible to trace back in IP address and practice there are too many mediating factors, including spoofing, dynamic IP, and other obfuscations. However at the packet level the packets carry information regarding the pathway they have taken. For example the ICMP protocol can hold information regarding at least the last two or three services it transacted through routers. Hence, in particular for mobile devices connected to a wireless router trace back progress can be made.

Table 3. Comparison of Traceback Methods

Traceback Method	Hop Count Filtering	ICMP	Logging	Marking	Marking & Logging	TTL & Marking	FDDA
ISP Involvement	None	Low	Moderate	Low	None	None	None
No. of Attack Packets needed for traceback	1	Very Large	1	Very Large	1	Very Large	large
Processing Overhead	Very Low	Low	Low	Low	Very Low	Low	High
Storage	Very Low	Low	Low	High	High	High	High
Ease of Implementation	Yes	Yes	Yes	No	No	No	No
Scalability	Highest	High	Fair	High	High	Highest	Highest
Bandwidth Overhead	None	Low	None	None	None	High	High
No. of functions needed to implement	3	2	3	2	5	5	6
Ability to handle major DDOS attack	Yes	Yes	Yes	Poor	Yes	Yes	Yes
Classification	IDS Based	Proactive	IDS Based	Proactive	IDS Based	Proactive	IDS Based
OSI Model Layer and Protocols	IP, Network Layer	ICMP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer	IP, Network Layer

The intermediate routers (routers between the source and destination) will generate a special ICMP packet according to the probability of 1 out of 20,000 once it receives an IP packet. The ICMP packet will be sent to either the source or the destination host with equal probability. The router's path information is stored in the ICMP packet and is collected and analyzed at the destination host. With forward or back link information, two routers can be identified in the path; while with two links of information, three routers can be identified. Because only partial path information is contained in the ICMP packet, it will be extremely difficult to identify several attack paths under a flooding DDoS attack but for slow attacks the method is much more effective (Kumar et al., 2010). To consistently construct the full or partial path, the destination host has to match the original IP packet with its corresponding ICMP packet, and this can be difficult. However, if the ICMP method is used in conjunction with the hop count method then some of the obstacles to tracing back to the source of the malicious packets can be overcome. The basic idea of hop count filtering method is to identify spoofed IP packets by using the source OS address and the hop count value in the IP packet and the filter of the spoofed IP packet under DoS and DDoS attack. The rational is that most of spoofed IP packets do not carry hop count values that are consistent with the IP address being spoofed at victim's device. Hence, an IP-to-hop-count (IP2HC) mapping table is built by the use of our metric during operations to distinguish between malicious and normal traffic. The simulation results show that close to 90% of spoofed traffic was identified (Paxson, 2001; Plohmann et al., 2011). Once an accurate IP2HC mapping table is built, the inspection algorithm checks the source IP address and the final time-to-live (TTL) value in each packet. The hop count method is not precisely an IP traceback method, since it cannot accurately pin point the attacking origin. It can only give a list of possible routers associating with an attacking origin. If all of the routers on the list form a circle, then the victim is the center and the hop count distance is the radius. Coupled with the ICMP analysis these are the most effective ways to trace back a slow DoS/DDoS attack (Smoeren et al., 2004).

CONCLUSION

Detecting and tracing slow attacks on mobile phone user services is possible when combinations of methodologies are employed. We have demonstrated using dummy attack data from the web (Table 2) that our metric will detect and alert a slow denial of service attack from any of the protocols in Table 1. The review of trace back methodologies shows that many are not useful for slow attack but a combination of ICMP and the hop count methodologies can be effective by simply focusing on the packets. Disruption and other attacks will continue to grow on mobile devices of any bandwidth. Consequently, further research is required into detection, protection, and trace back methodologies in order to secure services.

REFERENCES

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

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. 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.

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

Devasundaram, S. (2006).Performance evaluation of a TTL-based dynamic marking scheme in IP traceback. Akron, OH, USA: University of Akron.

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.

Gilad, Y., Herzberg, A.: LOT: A defense against IP spoofing and flooding attacks. ACM Transactions on Information and System Security, 15 (2), 6 (2012)

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

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.

Izaddoost, A., Othman, M, Rasid, M.: Accurate ICMP traceback model under DoS/DDoS attack. ADCOM '07 Proceedings of the 15th International Conference on Advanced Computing and Communications (pp. 441-446). Washington, DC, USA: IEEE Computer Society (2007)

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.

Kumar, B., Kumar, P., Sukanesh,: Hop count based packet processing approach to counter DDoS attacks . International Conference on Recent Trends in Information, Telecommunication and Computing (ITC) (pp. 271-273). Kochi, Kerala, India: IEEE (2010)

Kumar, K., Sngal, A., Bhandari, A.: Traceback techniques against DDoS attacks: A comprehensive review. 2011 2nd International Conference on Computer and Communication Technology (ICCCT) (pp. 491-498). Allahabad, India: IEEE (2011)

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

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

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.

Paxson, V.: An analysis of using reflectors for distributed denial-of-service attacks. ACM SIGCOMM Computer Communication Review, 31 (3), 38-47 (2001)

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

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.

Snoeren, A., Partridge, C., Sanchez, L., Jones, S., Tchakountio, F., Schwartz, B., Kent, S., Strayer, W. (2012). Single-packet IP traceback. IEEE/ACM Transactions on Networking, 10 (6), 721-734 .

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

Wang, H., Jin, C., Shin, K.: Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Transactions on Networking, 15 (1), 40-53 (2007)

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