Exploitation of ICMP Time Exceeded Packets for A Large-Scale Router Delay Analysis

Ali Gezer[1] and Gary Warner[2]
[1]Electronic and Telecommunication Technology, Kayseri University, Turkey
[2]Computer Science, University of Alabama at Birmingham, US

Abstract: *Internet Control Message Protocol Time-Exceeded (ICMP-TE) time exceeded packets are particular communication protocols to express inaccessibility of nodes in terms of hop count limitations. With the Internet of Things (IoT) concept taking more space in our daily life, accessibility or in some manners inaccessibility of hosts should be analysed more carefully. ICMP time exceeded packets might be hand of an attacker, sometimes an indicator of compromise for a possible IoT Botnet attack or a tool for delay measurement. In this study, with the exploitation of ICMP time exceeded packets, we analyse Round Trip Time (RTT) delays of randomly distributed IP routers around the globe. We conduct a comprehensive delay analysis study considering the delay results of more than 1 million time exceeded packets taken in return for subject ICMP requests. To prove ICMP time exceeded packets might also be a signature for a possible IoT Botnet attack, we carry out a secure experiment for Mirai IoT Botnet scanning and exhibit the indicators to differentiate these two possible usages.*

Keywords: *ICMP time exceeded packet, iot botnet, Mirai botnet, rtt delay, performance analysis, quality of service*.

Received April 19, 2018; accepted June 17, 2019

1. Introduction

Network measurements and traffic analysis play a vital role for network management and are a necessity for traceability of quality of service requirements to fulfil the growing needs of end users. Delay is one of the significant quality of service parameters for network performance measurement [18]. In a packet switched data communication process, many factors affect the total amount of packet delay such as propagation time, processing time, queuing time, and transmission time of packets. Other factors could add variations to delay such as network congestion, route changes, routing loops, etc. Delay also affects many mid-processes in the interaction of two end hosts over the Internet. For example, Transmission Control Protocol (TCP) uses a retransmission timer to ensure data delivery in the absence of any feedback from the remote data receiver [16, 21]. In [6], two new heuristics, autocorrelations and entropy of Round Trip Time (RTT) samples are introduced for TCP retransmission timeout calculations. TCP congestion control algorithm also utilizes RTT for congestion avoidance mechanism [2, 19].Understanding and modelling of end to end delays are also essential to design efficient routing algorithms, and dynamic resource sharing on the Internet.

With the growing popularity of Internet, delay measurement and characterization studies have increased in importance due to the expectation of better operation of Internet services. In [12], a large-scale round-trip delay time analysis for IPv4 hosts is carried out to observe how packet delay changes with geographical separations within 5 years. Mentioned study only analyses RTT delay of client hosts around the world. Fontugne *et al*. [10] analyses the relationship between the long range dependent parameter and the heavy tail parameter of the flow size distribution, and relates fine scale multifractal scaling to typical IP packet inter-arrival and to RTT distributions. Choi *et al*. [7] carried out a study about how to measure and report delay in a meaningful way for an ISP and how to monitor it efficiently. According to their study, reporting high quantiles in every 10-30 minutes is the most effective way to summarize delay for an ISP. This study only evaluates the packet delay between two taps on the same backbone link. Gürsun [13] studies the Internet delay space to detect anomalous routing paths via decomposing RTT delay space into components. Mentioned study obtained their measurement data from 47 Context Delivery Network (CDN) server nodes to 5076 client IPs located in France. The one-way delay and the round-trip delay are compared and contrasted through a wide selection of routers on the Internet via aiming the analysis of delay asymmetry on the Internet [20]. Unlike other studies, we perform a large-scale router delay measurement and analysis study with the usage of ICMP echo request to randomly selected IP hosts around the globe and ICMP Time Exceeded (ICMP-TE) packets taken in return for the subject ICMP requests. With the evaluation of more than 1 million ICMP TE packets, we obtain RTT delay results of 131.772 unique routers around the globe. In terms of its measurement approach, it is the first delay measurement study which takes into consideration

ICMP-TE packets taken in return for ICMP echo requests to inaccessible IP hosts.

Besides measurement purpose of ICMP-TE packets, they might shed lights upon abnormalities in TCP/IP communication. For example, routing loops are frequently encountered problems in the process of data communication over the Internet. Routing loops could be identified with the help of ICMP-TE packets. In some manners, ICMP-TE packets might be the hand of an attacker. An attacker might make use of ICMP-TE or ICMP destination unreachable packets by simply forging one of these ICMP messages and sending it to a communication host to break the connection [8]. ICMP-TE packets could also be exploited for a reflector attack by an attacker via sending data packets with a very low Time to Live (TTL) value. This event triggers routers to send time exceeded messages in return [5]. In [9], to debug networks where Multi-Protocol Label Switching (MPLS) is deployed, ICMP-TE packets are used by embedding an MPLS label stack in them. ICMP-TE packets are also exploited to infer the path properties. In [1], triggered stamping method was introduced to obtain information about a specific path.

ICMP-TE packets could also be a signature for identifying a possible Mirai IoT Botnet attack. The Internet of Things (IoT) has been the focus of much attention in the latter half of 2016 due to their broad exploitation in DDoS attacks, particularly in Mirai IoT Botnet [11]. Big Mirai Botnet attacks [17, 22] show that, accessibility or sometimes inaccessibility of Internet things should be analysed more carefully. During the scanning process of Mirai Bots, a great amount of IPv4 address space is scanned to discover new bots for forthcoming DDoS attack. In this process, obtained ICMP-TE packets could be a signature for the identification of Mirai Distributed Denial of Service (DDoS) attack in its early phase. We implement a secure experiment for Mirai IoT botnet via running a Mirai Bot for the IoT device scan. The signatures are obtained to identify the attack via the exploitation of ICMP-TE packets.

2. Measurement Data

Analysis of Network Traffic (ANT) Project Team [14] of Information Science Institute (ISI) has been probing all IPv4 addresses except some allocated ones such as multicast, private, loopback, class E addresses since 2003 to make censuses of Internet address space. One of the five chosen locations, Keio University in Kanagawa of Japan has been sending pings to all allocated IPv4 addresses through Widely Integrated Distributed Environment (WIDE) backbone network (AS 2500).The ICMP probe packets pass through WIDE's 150 Mbps incoming/outgoing transit Ethernet link to upstream ISP in Otemachi. Measurement and analysis on the WIDE Backbone (MAWI) [6] has been capturing the ongoing traffic on the link in 15 minute intervals via port mirroring technique and sharing the traces for research purposes through the Internet. This link carries both daily Internet traffic of WIDE backbone, intentionally generated abnormal traffic for research purposes, and ICMP packets of ANT research team.

IP addresses are anonymized, payloads are removed by tcpdpriv, and only the first 96 bytes are given for each packet in the shared traces. More than 100 million packets with a volume of nearly 30 GB traffic are captured in each 15 minute intervals. Captured traces consist of more than 40 application protocol traffic, and intentionally generated abnormal traffic. Each trace also includes approximately 23 million ICMP packets mostly belonging to ANT research project. For our study, we benefit from MAWI traffic archive to obtain the RTT delay statistics of routers scattered around the globe. Limited part of WIDE backbone network is illustrated in Figure 1.

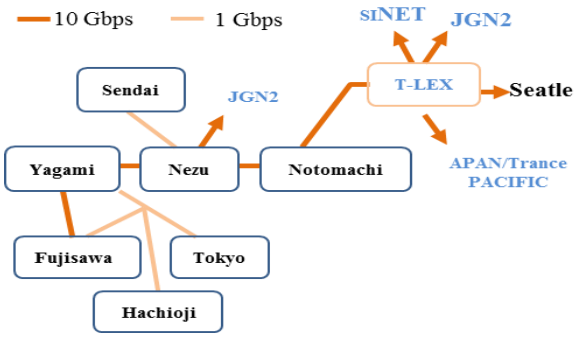

Figure 1. Part of WIDE network.

ISI's ICMP probe sends ICMP request messages to each address in the IPv4 allocated space and waits for reply. A positive reply means that the sending host takes ICMP reply packet from the destination host. Approximately, 4 million ICMP requests take ICMP reply in 15 minutes. Most of the ICMP requests don't take any reply due to a firewall or unreachability of the host at that specific time. Because of the privacy of individual IP addresses, MAWI anonymize IP addresses with a prefix-preserving method and prefix mapping is consistent among the traces. A significant number of routers send ICMP-TE messages to the source host which means your packet doesn't reach its destination after passing through a certain number of hops. At the capturing point (NTT Otemachi Building), ICMP requests have a TTL value of 59. When an ICMP-TE is obtained for this ICMP request, it means that the ICMP request packet could not reach its destination after passing through 59 hops. In total, 1.230.144 ICMP-TE packets are obtained and evaluated for the delay analysis in this study.

3. Methodology

Considering the abundance of many application

protocol packets and ICMP packets in each trace file, it is a troublesome operation to match ICMP-TE messages with their correspondent ICMP requests and obtain the RTT delay values of routers. To carry out the process, the following methodology is implemented for each trace file via the exploitation of some fields in ICMP packets. A standard ICMP packet format is illustrated in Figure 2 and some ICMP types are given in Table 1.

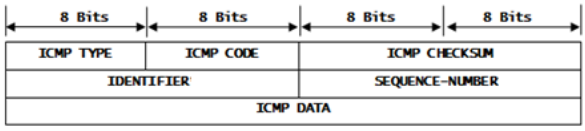

Figure 2. ICMP frame format.

Table 1. ICMP type codes.

Type	Message
0	Echo Reply
3	Destination Unreachable
5	Redirect
8	Echo Request
11	Time exceeded

Only filtering ANT related packets, we determine the IP address of pinging ISI's probe. Because of the scrambling policy of IP addresses by MAWI, located IP addresses don't point out the real IPs. But it doesn't make any difference for our study due to the preserved IP mapping consistency among the traces. To filter only ICMP-TE packets belonging to ANT project, the following filter is applied in wireshark protocol analyser.

(icmp.type == 11 and ip.dst==”ISI's ICMP probe”)

Table 2. Extracted fields from ICMP-TE frames.

Fields
Identifier
Sequence
Capture time of the Frame
Time to Live Value
Source IP of ICMP-TE packet
IP address of ICMP Request in ICMP-TE Packet

To extract required fields from ICMP-TE frames, we develop a software solution in Microsoft Visual Studio. The developed scraping application extracts the information in Table 2 from exported text files which has more than 12 million rows. Then, the following filter is applied to obtain non-reply ICMP request packet details.

(icmp.type==8 and !icmp.resp_in and ip.src==”USC' s host IP”)

Approximately 13 million ANT related non-reply ICMP request packets are obtained for each trace file. Considering all filtering operations, and scraping processes, it takes approximately 25-30 hours to get associated ICMP request and ICMP-TE fields in two separate tables for a single trace file with Intel Core i7-3770 CPU 3.40 GHz, 16 MB RAM desktop computer.

After importing the extracted information of ICMP-TE and ICMP request packets as two separate tables into a database application, some pre-processing operations are performed to prepare the data for matching. Pairing of packets is provided if only IP address, identifier and sequence number are all matched in the ICMP-TE and ICMP request packets.

4. Delay Analysis

48-hour long traffic are captured in 15 minute intervals during December 2nd and 3rd, 2015 and shared in WIDE archive. According to the analysis results of 00.00-00.15 December 2nd, 2015 trace, 86.346.195 packets are captured through 150 Mbps WIDE backbone link and 22.764.400 (26.36%) of them are ICMP packets mostly belonging to ANT project. It includes ANT related, 7.898.192 matched ICMP request–reply ICMP packets, 12.243.035 non-reply ICMP request packets and 200.850 ICMP-TE packets. After carrying out the filtering and the data processing operations following the methodology given in the previous section, 167.804 packet pairs are obtained which refers to some non-reply ICMP requests take ICMP-TE messages due to the hop count limitation. Moreover, some request packets take more than one ICMP-TE messages and vice versa. To make the analysis more reliable, we only filter the ICMP request packets whose destination address is unique. For the mentioned trace, 134.951 unique matchings are obtained. Similar steps are performed for other traces and summary information is given in Table 3.

Table 3. Summary information of analyzed traces.

Date-Time İnterval	Total ICMP Packets	ICMP-TE Packets	Match. Counts	Unique Match.	Uniq Source
12.02.2015 00.00-00.15	22.764.400	200.850	167.804	134.951	21.635
12.02.2015 00.15-00.30	26.415.27	205.199	168.923	133.950	21.601
12.02.2015 06.00-06.15	22.669.770	196.499	170.097	139.801	21.779
12.02.2015 12.00-12.15	24.556.763	237.149	221.637	148.577	23.271
12.02.2015 18.00-18.15	23.929.802	187.649	155.574	134.189	21.651
12.03.2015 00.00-00.15	24.036.063	202.798	182.979	133.134	21.835

There is also one significant point which has drawn attention in our analysis; some addresses generate excessive number of time exceeded messages for separate ICMP requests. For instance, one particular IP address generates 4.551 ICMP-TE messages for separate ICMP requests. The following two IPs generate 3.166 and 2.768 ICMP-TE messages. Via a deeper analysis, it is seen that mentioned routers mostly raise time exceed messages to requests whose IP addresses have the same prefix; only the suffix part differs. Summary information about time exceeded repetitions is given in Table 4. To avoid repetitions in similar cases, average delay is calculated if the source

addresses of time exceeded packets are the same. After this operation, 21.635 distinct pairings are obtained for the mentioned trace. The obtained results for other traces are shown in the last column of Table 3.

Table 4. Repetitions of ICMP-TE messages for the same IP routers.

12.02.2015	Source IP	Count	Mean Delay	TTL
00.00-00.15	212.18.104.85	2768	0.23949	247
	41.207.224.201	3166	0.42556	56
	195.202.44.14	4551	0.28848	52
00.15-00.30	212.18.104.85	2608	0.23516	247
	41.207.224.201	3150	0.41216	57
	195.202.44.14	4367	0.28263	52
06.00-06.15	212.18.104.85	2347	0.23436	247
	41.207.224.201	3130	0.42489	57
	195.202.44.14	4345	0.28156	53
12.00-12.15	212.18.104.85	2629	0.24433	247
	41.207.224.201	3118	0.43399	57
	195.202.44.14	4315	0.29168	53
18.00-18.15	212.18.104.85	1712	0.33063	243
	41.207.224.201	3167	0.42511	57
	195.202.44.14	4165	0.28184	53

The studies on delay suggest that the delay metric should indicate the quantity of delay experienced by most packets in the network, capture anomalous changes and not to be sensitive to statistical outliers [4, 15]. According to the [7], reporting high quantiles (between 0.95 and 0.99) is the most effective way to summarize delay. We adopt the same approach to eliminate the statistical outliers and focus on the delay quantity which most of the routers experienced. For the mentioned trace file, 95% percent of packets experience delay less than 0.7801 second delay. Using this information, we exhibit the delay values of routers in between 0-1 second interval as shown in Figure 3. This graphic exhibits the RTT delays between the capturing router at Notemachi and the mid-routers around the world which send ICMP-TE packet when TTL value of ICMP request reaches 0. Every point represents a delay point of a separate router.

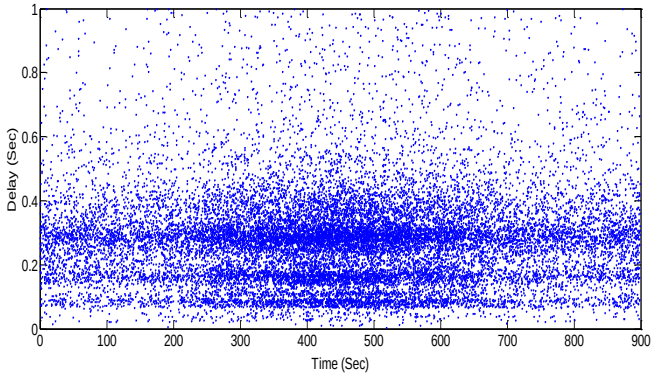

Figure 3. RTT delay values up to 1 second between the capturing routing and mid-routers (December 2nd, 2015, 00.00-00.15).

It could be observed that there are three concentrations at delay points below 0.4 second. The frequency distribution of RTT delays make this extraction more obvious as shown in Figure 4. To eliminate statistical outliers, representation only includes delays up to 0.8 second. Considering some request packets don't reach their destination after traveling 59 hops and taking into account the return time of time exceeded messages, most of the requests complete their journey in less than 0.5 second.

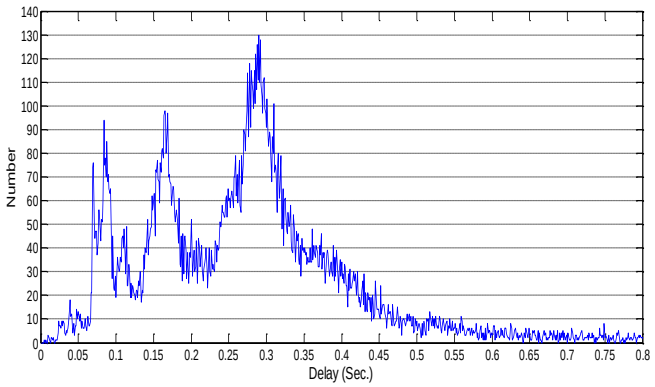

Figure 4. The RTT frequency distribution of routers with 1 ms. bin size (December 2nd, 2015, 00.00-00.15).

In Figure 5, similar distributions are obtained for 4 separate traces with 10 ms. resolution in the same date which differ each other by 6 hours. Although delay behaviour of close routers to the capturing point change remarkably, remote ones don't change much. However, choosing close time intervals don't affect the delay behaviour seriously, and gives nearly same distributions as could be seen in Figure 6.

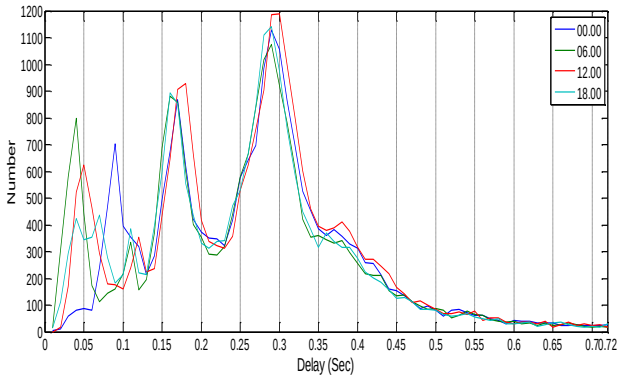

Figure 5. Frequency distribution of RTT delays in different time intervals with 0.01 Sec. resolution(December 2nd, 2015).

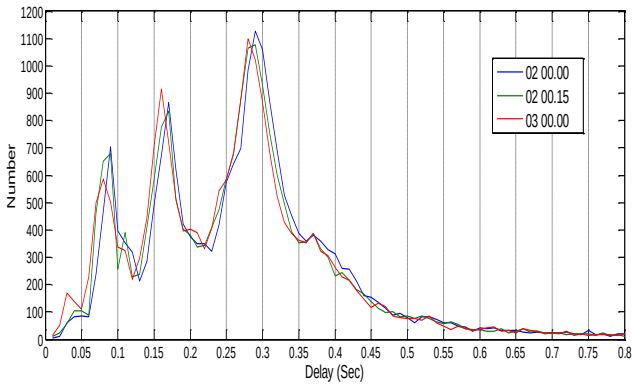

Figure 6. Frequency distribution of RTT delays in close time intervals with 0.01 sec. resolution.

We cannot track the location of IP addresses due to IP anonymization policy of MAWI. But the wavy form

of all distribution figures shows that, there must be clustering of routers in different locations of the world. Differences might be caused by continental, territorial or regional separations. This kind of waviness preserves itself in other day traces, also.

In Figure 7, the TTL counts of time exceeded messages are exhibited for 00.00-00.15 trace. Although, some ICMP request packets could not reach their destination after travelling 59 routers, most of the time exceeds packets reach the capturing point through only a few hops. Generally, routers generate ICMP packets with 64, 128 and 256 TTL according to their Internetwork Operating Systems (IOS). Concentration of hosts close to the mentioned TTL values at the capturing point proves that the return way includes only a few hops. This graphic shows that some of the request packets experience rooting loops, and in these loops, they consume their hop count limit.

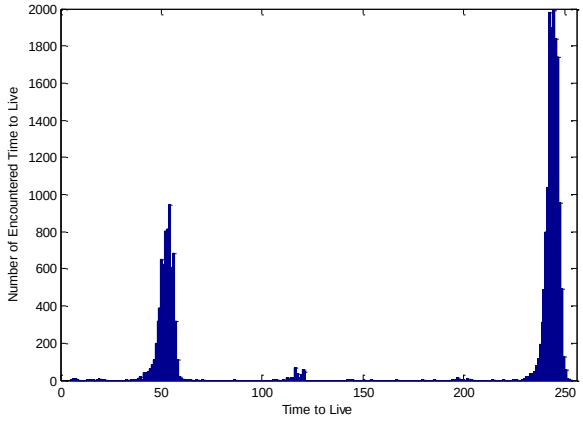

Figure 7. TTL counts of ICMP-TE packets (December 2nd, 2015, 00.00-00.15).

Figure 8 exhibits how time exceeded delay varies with the TTL value. The aggregation on 64, 128 and 256 is caused by most of router IOS generate Internet Control Message Protocol Time-Exceeded (ICMP-TE) packet with 64, 128 and 256 TTL value. Via inspecting concentration points, average delay decreases with respect to TTL increment.

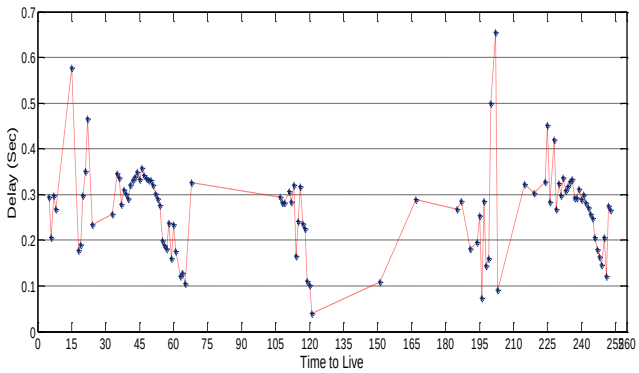

Figure 8. Delay variation with respect to TTL (December 2nd, 2015, 18.00-18.15).

5. ICMP-TE Packets as an Indicator for Mirai IoT Bots Scanning Attack

MiraiIoT Botnet started drawing attention in the second half of 2016 [11] due to its contribution in large DDoS attacks. The first big incident was the attack to the website of security journalist Brian Krebs with an exceeded 600 Gbps traffic in volume on September 21st, 2016 [17]. Nearly at the same dates, French webhost and cloud service provider OVH was hit with a hit 1.1 Tbps traffic [22]. A month later, Dyn internet service provider was targeted with an estimated 1.2 Tbps [17] that took down hundreds of websites-including Twitter, Netflix, Reddit, and GitHub. The mentioned DDoS cyber-attacks were both attributed to Mirai Botnet. Mirai created an army of routers, embedded and IoT devices through login them via guessing their weak or factory settings credentials and force them to download and execute malware binaries to make them a Mirai Bot. Due to their constrained-resources, specific protocol stacks and standards, IoT devices are subject to security vulnerabilities and attacks [23].

We focus on Mirai's scanning process for IoT bots due to the similarities between it and the scanning phase of IPv4 address space applied in this study. Mirai bots scan IPv4 address space for possible IoT devices that run Telnet or SSH via TCP SYN probes. Bots attempt to log in to these devices through a TCP connection on Telnet ports 23 and 2323 using a hardcoded dictionary of IoT credentials mostly comprised of weak and factory default user names and passwords. During brute-force login phase, 10 username and 10 password pairs chosen randomly from a pre-configured list of 62 credentials are tried [3]. When a successful login happens, the bot sent the IP address and associated credentials of the IoT device to a report server. Mirai actors and their roles are illustrated in Figure 9.

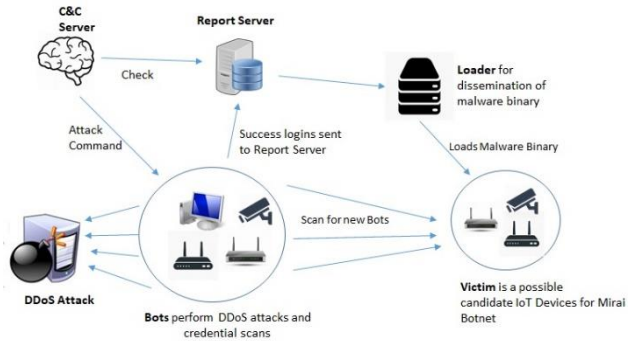

Figure 9. Mirai components.

In this study, we implement an experimental setup to prove that ICPM-TE packets could be an indicator for IoT botnet attack. For our implementation, we setup a virtual machine environment to execute Mirai malware binary for IoT Botnet scanning. For the safety of IoT devices and not to contribute a possible IoT

DDoS attack, we cut the communication between our Mirai Bot, and the Reporter through redirecting DNS query of Reporter (www.santasbigCandycane.cx) to our local machine. Thus, victim IoT device credentials would not be shared with Mirai Reporter and the integrity of Mirai is broken. Our implementation for Mirai Bot scanning is illustrated in Figure 10.

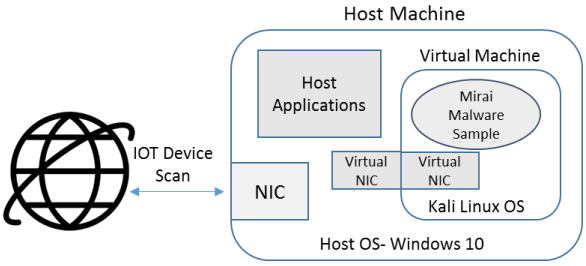

Figure 10. Our implementation for running Mirai sample in secure environment.

After running Mirai binary sample in Virtual Machine and turning our Virtual Machine into a Mirai Bot, we capture the network traffic using Wireshark protocol analyzer. At the end of 40 minutes scanning, 763.600 IPv4 address are scanned via TCP SYN on Telnet port TCP 23 and TCP 2323. Approximately 600 hosts setup TCP connection on Telnet port with our virtual machine and brute force login phase is initialized. 145.754 ICMP-TE packets are captured in scanning phase due to hop count limitation. Our box sent TCP SYN packet with a 64 TTL value. A great number of ICMP-TE packets occurred due to a quick IoT Bot scanning process. Comparison of ICMP-TE packets in delay measurement study and IoT Botnet scanning give us some signatures to differentiate these two possible occurrences. Obtained signatures are given in Table 5.

Table 5. Signatures in ICMP-TE packets.

	Delay Measurement	**Mirai IoT Bot Scan**
Packet Length	Mostly 70 Bytes Rarely 74, 110, and 182 bytes	Mostly 110 Bytes Rarely 70 Bytes
Original Datagram	ICMP Echo Request	TCP SYN packet

6. Discussion and Limitations

For the router delay statistics study, we benefit from the traffic traces archive of WIDE which also include ICMP packets of the ANT project team for their IPv4 address censuses research study. The main reasons for the selection of mentioned traffic traces is long measurement period and high number of IPv4 hosts existence in the traces. Although many contributions of WIDE traces into our study, they also restricted our measurements in some ways. Due to IP address anonymization policy of MAWI, we could not track the IPv4 address locations, and point out the delay differences of specific locations to the measurement point. In our future studies, we plan to overcome this restriction via designing a ping tool. We believe that, the designed tool would make valuable contributions to the findings of this study and might provide us with new insight into the topic.

We are planning to perform further analysis on Mirai Botnet and other IoT Botnet families such as Satori, QakBot, Hakai, Mirai, etc. via executing associated malware binaries on virtual machines. Static and dynamic analysis will be performed on malware binaries to get more insights and indicators about them. The results of analysis will provide some ground truth information about their effects, and also overcome the difficulties regarding with them. They may also provide significant information about the possible forthcoming IoT Botnet DDoS attacks in the future. IoT Botnet attacks need IoT device scan to infect more IP hosts and enlarge their bot army. In this process, ICMP related packets, such as ICMP reply, ICMP network unreachable, ICMP host unreachable, and ICMP time exceeded messages may consist valuable indicators about particular IoT Botnet attacks. We will focus on the analysis of other ICMP types with the aim of detecting IoT Botnet attacks in our future studies.

7. Conclusions

This study evaluates the delay statistics of routers to a vantage point with the exploitation of ICMP-TE packets of unreachable hosts around the world. There are some concentrations in delay points between 0.16-0.19 and 0.27-0.31 seconds in terms of number of host numbers. The frequency distribution of routers below 0.1 second is affected with different time intervals in a day. Another interesting result in our analysisis that, some routers generate a high number of time exceeded messages to different ICMP requests. In this manner, mostly ICMP requests differ between each other with the suffix part of the destination IPs, the prefix parts are generally same. Although ICMP requests could not reach their destination after 59 hops, the return way of ICMP-TE packets includes only a few hops. It demonstrates that many ICMP request packets experience rooting loop, and they consume their hop count limit in the routing loops. ICMP-TE packets might also be indicator of cyber attacks. In Mirai IoT Botnet scanning, a great number of ICMP-TE packets occurred for unreachable hosts in a short period of time. It is demonstrated that to identify Mirai IoT Bot net attacks in its early phase, packet length and original datagram of ICMP-TE packets could be used as a signature.

Acknowledgement

I would like to thank Dr. Murat M. Tanık and Dr. Thomas Hinke for their support, and guidance. I appreciate Mustafa İlhan for his contribution to this study. I also would like to thank Michael Mistretta for helping in the review of the study.

References

[1] Allman M., Beverly R., and Trammell B., "Principles for Measurability in Protocol Design," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 2, pp. 2-12, 2017.

[2] Allman M., Paxson V., and Blanton E., "TCP Congestion Control," *IETF RFC 5681*, 2009.

[3] Antonakakis M., April T., Bailey M., Bernhard M., Bursztein E., Cochran J., Durumeric Z., Halderman J., Invernizzi L., Kallitsis M., Kumar D., Lever C., Ma Z., Mason J., Menscher D., Seaman C., Sullivan N., Thomas K., and Zhou Y., "Understanding the Mirai Botnet," *in Proceedings of 26th USENIX Security Symposium*, Vancouver, pp. 1093-1110, 2017.

[4] Boutremans C., Iannaccone G., and Diot C., "Impact of Link Failures on VOIP Performance," *in Proceedings of Network and Operating Systems Support for Digital Audio and Video*, Miami, pp. 63-71, 2002.

[5] Chang R., "Defending Against Flooding-Based Distributed Denial of Service Attacks: A Tutorial," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 42-51, 2002.

[6] Cho K., Mitsuya K., and Kata A., "Traffic Data Repository At The WIDE Project," *in Proceedings of the Annual Conference on USENIX Annual Technical Conference*, San Diego, pp. 263-270, 2000.

[7] Choi B., Zhang Z., Hung D., and Du C., Scalable Network Monitoring in High Speed Networks, Springer, 2011.

[8] Chowdhary M., Suri S., and Bhutani M., "Comparative Study of Intrusion Detection System," *International Journal of Computer Sciences and Engineering*, vol. 2, no. 4, pp. 197-200, 2014.

[9] Donnet B., Luckie M., Merindol P., and Pansiot J., "Revealing MPLS Tunnels Obscured from Traceroute," *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 2, pp. 87-93, 2012.

[10] Fontugne R., Abry P., Fukuda K., Veitch D., Cho K., Borgnat P., and Wendt H., "Scaling in Internet Traffic: A 14 Year and 3 Day Longitudinal Study, with Multiscale Analyses and Random Projections," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2152-2165, 2017.

[11] Gannon M., Warner G., and Arora A., "An Accidental Discovery of Iot Botnets and A Method for Investigating Them with A Custom Lua Dissector," *in Proceedings of Conference on Digital Forensics, Security and Law. 3*, Daytona Beach, 2017.

[12] Gezer A., "Large-Scale Round-Trip Time Analysis of Ipv4 Hosts Around the Globe," *Turkish Journal of Electrical Engineering and Computer Sciences*, vol. 27, no. 3, pp. 1998-2009, 2019.

[13] Gürsun G., "On Spectral Analysis of Internet Delayspace and Detecting Anomalous Routing Paths," *Turkish Journal of Electrical Engineering and Computer Science*, vol. 27, no. 2, pp. 738-751, 2019.

[14] Heidemann J., Pradkin Y., Govindan R., Papadopoulos C., Bartlett G., and Bannister J., "Census and Survey of the Visible Internet," *in Proceedings of 8th ACM SIGCOMM Conference on Internet Measurement*, Vouliagmeni, pp. 169-182, 2008.

[15] Hengartner U., Moon S., Mortier R., and Diot C., "Detection and Analysis of Routing Loops in Packet Traces," *in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement*, Marseille, pp. 107-112, 2002.

[16] Janowski R., Grabowski M., and Arabas P., "New Heuristics for TCP Retransmission Timers," *in Proceedings of International Conference on Computer Recognition Systems, Progress in Computer Recognition Systems*, Cham, pp. 117-129, 2019.

[17] Kolias C., Kambourakis G., Stavrou A., and Voas J. "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80-84, 2017.

[18] Mohammed H., Attiya G., and El-Dolil S., "New Class-based Dynamic Scheduling Strategy for Self-Management of Packets at the Internet Routers," *The International Arab Journal of Information Technology*, vol. 16, no. 3, pp. 473-481, 2019.

[19] Mudassar A., Asri N., Usman A., Amjad K., and Ghafir I., "A New Linux Based TCP Congestion Control Mechanism for Long Distance High Bandwidth Sustainable Smart Cities," *Sustainable Cities and Society*, vol. 37, pp. 164-167, 2018.

[20] Pathak A., Pucha H., Zhang Y., Hu Y., and Mao M., "A Measurement Study of Internet Delay Asymmetry," *in Proceedings of International Conference on Passive and Active Network Measurement*, Cleveland, pp. 182-191, 2008.

[21] Paxon V., Allman M., Chu J., and Sargent M., "Computing TCP's Retransmission Timer," *IETF RFC 6298*, 2011.

[22] Sinanovic H. and Mrdovic S., "Analysis of Mirai Malicious Software," *in Proceedings of 25th International Conference on Software, Telecommunications and Computer Networks*, Spli, pp. 1-5, 2017.

[23] Zarpelao B., Miani R., Kawakani C., and Alvarenga S., "A Survey of Intrusion Detection

in Internet of Things," *Journal of Network and Computer Applications*, vol. 84, pp. 25-37, 2017.

Ali Gezer was born in Kayseri City, Turkey, in 1976. He received the B.S. degree in Electronic and Computer Education from Marmara University in 1999 and M.S. degree in Computer Engineering from Erciyes University in 2004, and the Ph.D. degree in Electronic Engineering from Erciyes University, Kayseri, TURKEY, in 2011. He is an assistant professor with the Electronic and Communication Technology in Kayseri University. His research interests include internet traffic analysis, self-similarity, network traffic modelling and characterization, signal processing techniques, telecommunication technologies, IoT botnet investigations, and malware analysis.

Gary Warner was born in Indiana and grew up in the Mid-West. He moved to Birmingham, Alabama to attend UAB, where he earned his Bachelor's in Computer Science. Warner has worked in mainframe operations, network security and design, and as the I.T. Director for an oil and gas company. He started the Birmingham InfraGard chapter in 2001, and has served on the national board of directors for both the FBI InfraGard program and the DHS Energy ISAC. In 2007, he joined the University of Alabama at Birmingham to train future cybercrime investigators. He currently directs a staff of 50 student researchers in the UAB Computer Forensics Research Lab where he works primarily on malware and botnet investigations, cybercrime investigations, and the social media usage of criminals, hate groups, and terrorists.