A NOVEL APPROACH TO PROVIDE SECURITY MECHANISM TO COUNTER DDOS ATTACKS USING BLOCK CHAIN TECHNOLOGY

[1]N. Aruna,[2] T. Dohala,[3] V. Praneetha,[4]V. Niharika,[5]M. Srinivasa Rao

[1,2,3,4] B.Tech Scholars, Dept. of CSE, Sri Vasavi Institute Of Engineering and Technology,

Nandamuru AP India.

[5]Professoor, Dept of CSE, Sri Vasavi Institute Of Engineering and Technology,

Nandamuru AP India.

Abstract: The Internet of Things or IoT is a rapidly growing phenomenon. Many of the devices around us are getting connected to the Internet, becoming "smart" in the process. However, increased connection to the Internet invites possible cyber-attacks from multiple directions. One of the fundamental problems of IoT devices is that they are bought and deployed in batches. Therefore, a majority of IoT devices deployed remain with the default factory assigned username/password combination as the only means for authentication. These makes it very easy to bruteforce into these devices and take control of them. The Mirai botnet attack that took down the Dyn DNS and consequently many other important sites last October used a DDoS attack. The attack formed its botnet by brute forcing into IoT devices using default username and password combinations. One way to protect against this kind of brute force attack is to use key-based authentication as well for encrypted communication among IoT devices. This work proposes multiple architectures and protocols to enable key-based authentication for IoT devices, leveraging the block chain technology. This work also describes a scalable simulator in NS3 to test IoT specific public key infrastructure on block chain and corresponding communication protocols.

IndexTerms **– Blockchain; Cryptography; Internet of Things; DDOS Attacks; Mirai System;**

1. INTRODUCTION

Internet of things (IoT) is a digital ecosystem which provides the capability of inter-connectivity among the physical devices. Organizations around the world comprehend the impact of socio-economic potential of IoT and are eagerly exploring how their economies might raise benefits from various sectors, such as healthcare, infrastructure management and utilities. In order to achieve the goal of inter-operability among devices using device-to-device communication technologies that make up the digital ecosystem, cooperation among these organizations involved in IoT development is required. The number of connected devices has now exceeded the world population and Gartner predicts that around 20 billion Internet-connected devices will be in use by 2020.

From the very beginning, the issue of security in IoT has been its soft spot and tremendous efforts have been made by both industry and academia to overcome it. Attackers show much interest in IoT devices as compared to traditional devices due to the fact that they hold sample amount of sensitive data and are vulnerable to simple attack attempts. Recent studies show the threat of IoT devices getting compromised in masses. Due to diverse and unified nature of IoT networks, new devices entering the

network are configured automatically and are highly prone to security attacks. Lack of standardization is one of the reasons of vulnerabilities in IoT devices. Companies involved in manufacturing these devices are in a rush to occupy more space in the digital market. If vulnerability in the IoT device is found by the manufacturer and if the patch is released, it might not be easier to upgrade some of the devices but still the whole system is in safe state. However, if the same vulnerability is found by the attacker and the attacker compromises that particular device before the release of its patch, it becomes the responsibility of the manufacturer to release and apply the patch by informing the user about that device. Fig. 1.1.1 shows the vulnerability cycle in IoT devices. Several other issues that are equally responsible for the breach of IoT security are limited power, storage capacity and computational capabilities of the IoT devices. Shorter passwords, difference in storage formats, data processing methods, security control mechanisms and data filtering techniques also give rise to various security challenges, due to which it becomes difficult to establish privacy, trust, confidentiality, authentication and access control in the whole system (Fig. 1.1.2). One such security challenge is detection and prevention of **Distributed Denial of Service (DDoS)** attack over IoT devices which are becoming a hefty threat. It involves a group of geographically distributed zombie computers that interrupt and block legitimate users by flooding the host server or the communication channels with huge number of requests within a network. To overcome this problem, numerous solutions have been proposed in the past depending upon the type of network infrastructure and application.

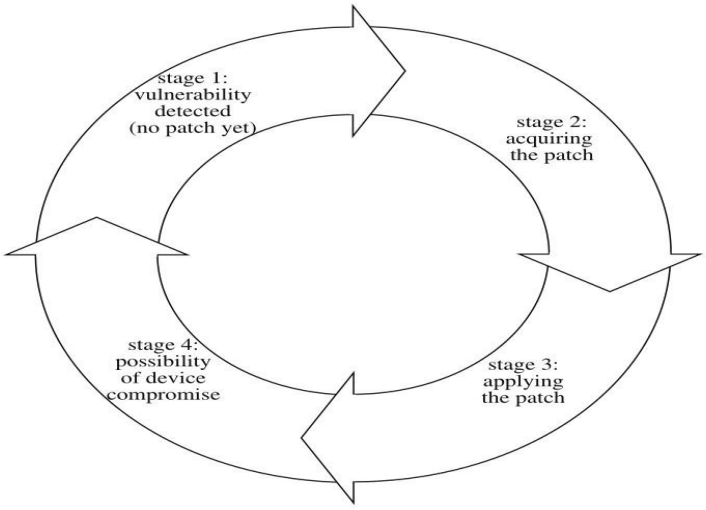


Fig. 1.1.1 Vulnerability Cycle in IoT Devices

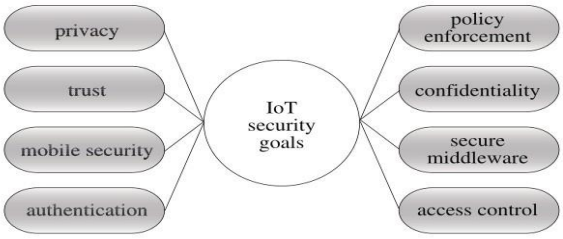
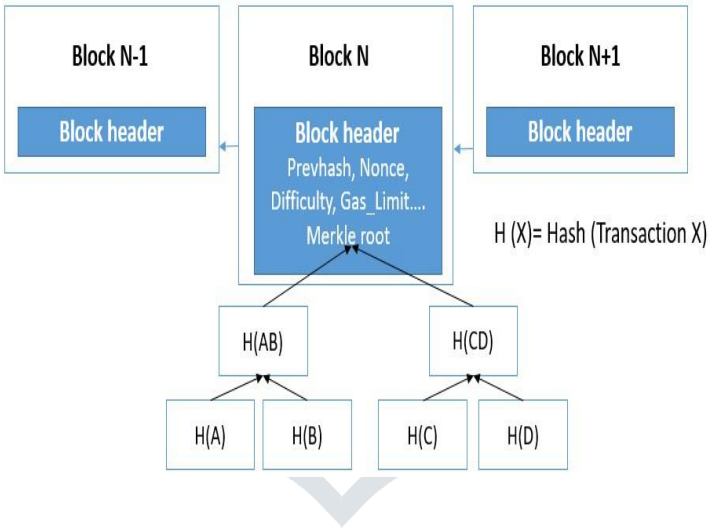


Fig.1.1.2 Security Goals in IoT

2. BLOCK CHAIN TECHNOLOGY:

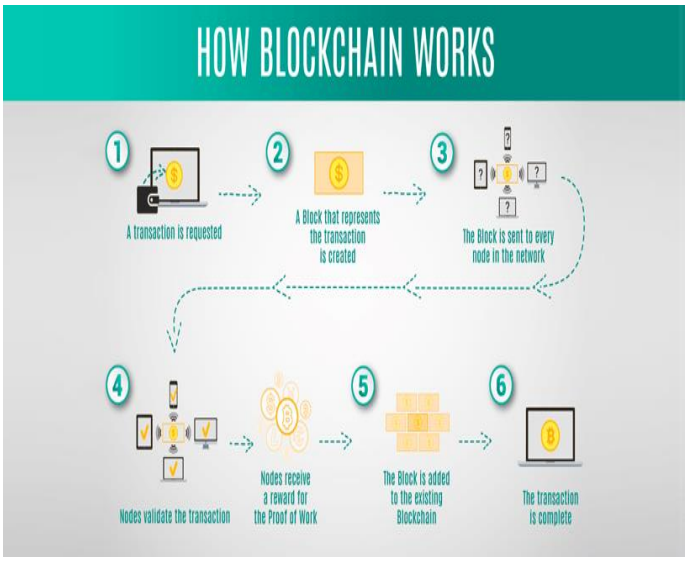
As of late, digital currency has pulled in broad considerations from both industry and the scholarly world. Bitcoin that is regularly called the primary digital money has delighted in a colossal accomplishment with the capital market achieving 10 billion dollars in 916. The block chain is the center instrument for the Bitcoin. Blockchain was first proposed in 908 and executed in 909 . Block chain can be viewed as an open record, in which every single submitted exchange are put away in a chain of blocks. This chain consistently develops when new blocks are annexed to it. The blockchain innovation has the key qualities, for example, recentralization, persistency, namelessness and auditability. Blockchain can work in a decentralized situation, or, in other words coordinating a few center innovations, for example, cryptographic hash, computerized signature (in view of hilter kilter cryptography) and circulated accord system. With blockchain innovation, an exchange can occur in a decentralized manner. Thus, blockchain can significantly spare the expense and enhance the productivity.

Blockchain is an arrangement of blocks, which holds a total rundown of exchange records like customary open record. Each block indicates the promptly past block by means of a reference that is basically a hash estimation of the past block called parent block. It is significant that uncle blocks (offspring of the block's precursors) hashes will likewise be put away in ethereum blockchain. The main block of a block chain is called beginning block which has no parent block.



How the Blockchain networks will work:

The Bitcoin organize is a circulated system where carefully marked exchanges are kept up by an open record speaking to similar information. With the end goal to interrelate with the blockchain, an exchange is communicated into the system and approved by all companions. A block holds the data identified with every exchange and once an agreement is accomplished, the block will be affixed the blockchain. The procedure will begin once again for each new exchange.



3. DDOS ATTACKS:

An attacker executes denial of service (DoS) attack in order to consume the resources, such as bandwidth of a service provider so that a legitimate user in the network is not able to use those services and suffers in terms of delayed responses or frequent network failures. This attack achieves its goals by streaming packets that diminish the processing capability of the network, as a result denying access to the legitimate users.

DDoS attacks are elaborated form of DoS attacks and hence more advance where multiple attacking nodes and network connections are involved. As a result, huge number of malicious packets or bad requests are generated that can easily cause disruption of the services and breakdown of the target network. To distinguish between legitimate packets and attack packets is arduous, as the traffic is usually so aggregated that there are no probable characteristics of the DDoS stream that could be idiosyncratically used for prevention and detection of the attack. In simple words, DDoS attack involves the same service being targeted by multiple inter-connected attacking devices.

DDoS attack does not rely on particular network protocol or system weakness. It simply exploits the huge resource asymmetry between the Internet and the victim. Since Internet architecture is open in nature, any machine attached to it is publically visible to another machines attached to enable the communication. The hacker or attacker community takes the unhealthy advantage of this open nature to discover any insecure machine connected to the Internet. The discovered machine is thus infected with the attack code. The infected machine can further be used to discover and infect another machine connected and so on. The attacker thus gradually prepares an attack network called botnet. Depending upon the attacking code the compromised machines are called Masters/Handlers or zombies. Hackers send control instructions to masters, which in turn control zombies. The zombies under the control of masters/handlers transmit attack packets as shown in Fig. 4.1, which converge at victim to exhaust its resources. DDoS attack basically targets victim's computational or communicational resources , such as bandwidth, memory, CPU cycle, file descriptors and buffers etc.

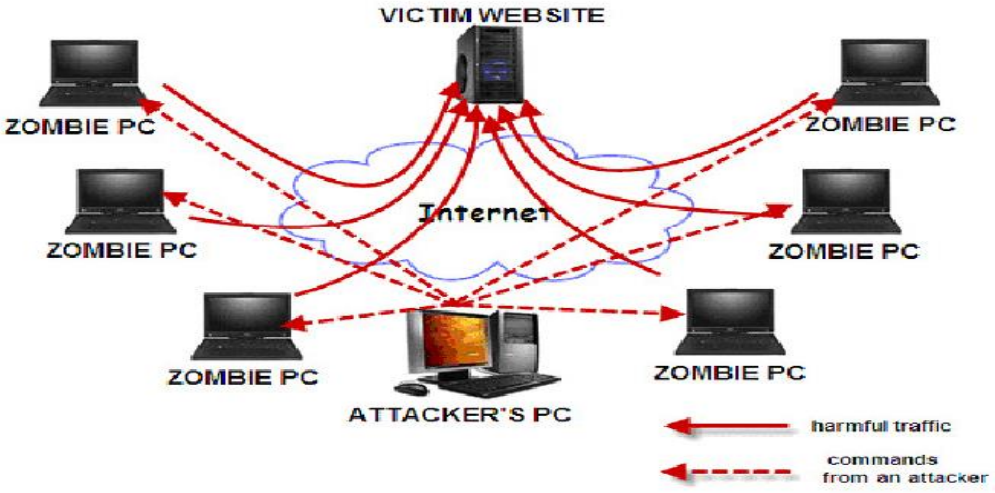


Fig 3.1 DDOS Attack Architecture

3.1. MIRAI SYSTEM:

Mirai is malicious software that creates botnet of IoT devices. It drew public attention in September 2016 after it was used in DDoS attack against Kerbs On Security website which reached 620 Gbps. Mirai is a piece of malware that infects IoT devices and is used as a launch platform for DDoS attacks.

Mirai is built for two core purposes:

- Locate and compromise IoT devices to further grow the botnet.
- Launch DDoS attacks based on instructions received from a remote C&C.

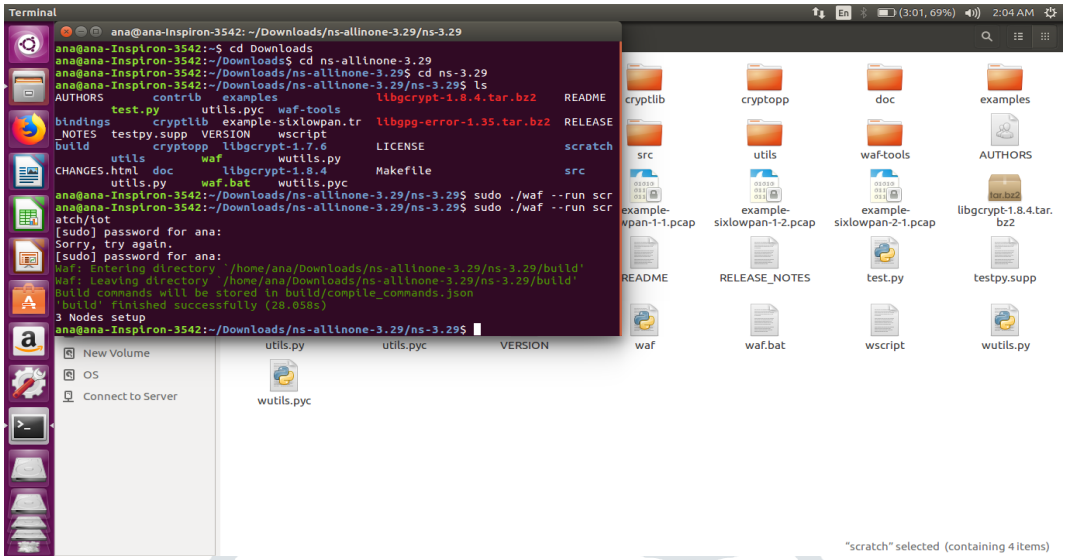
Mirai is a self-propagating botnet virus. The source code for Mirai was made publicly available by the author after a successful and well publicized attack on the Krebs Web site. Since then the source code has been built and used by many others to launch attacks on internet infrastructure. The Mirai botnet code infects poorly protected internet devices by using telnet to find those that are still using their factory default username and password. The effectiveness of Mirai is due to its ability to infect tens of thousands of these insecure devices and co-ordinate them to mount a DDOS attack against a chosen victim.

3.2. NS3 (NETWORK SIMULATOR-3):

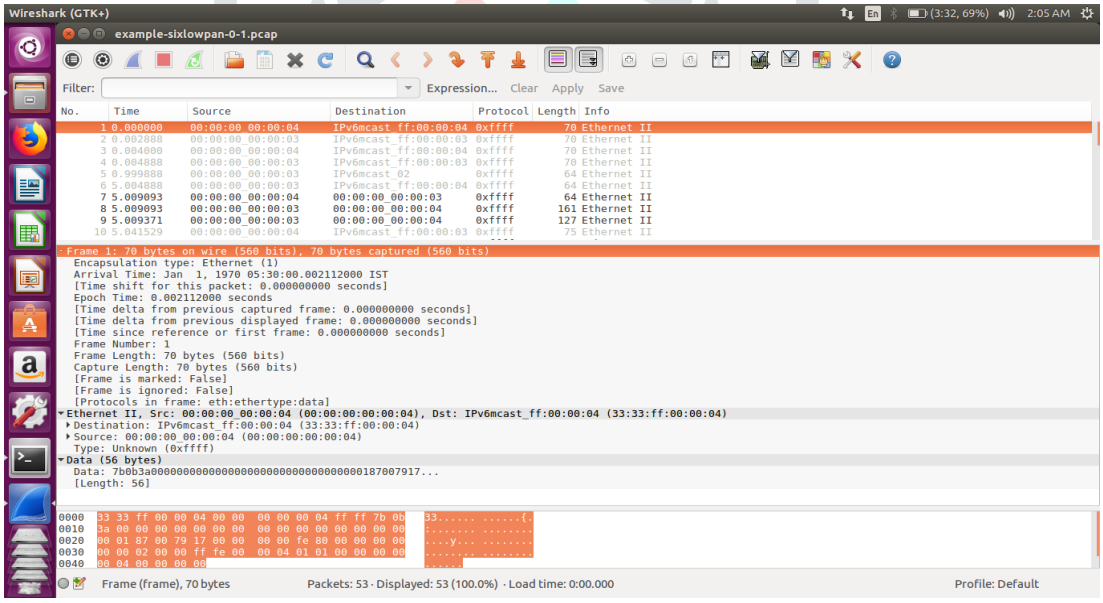
The *ns-3* simulator is a discrete-event network simulator targeted primarily for research and educational use. The ns-3 project, started in 2006, is an open-source project developing *ns-3*.

- *ns-3* is open-source, and the project strives to maintain an open environment for researchers to contribute and share their software.
- *ns-3* is not a backwards-compatible extension of ns-2; it is a new simulator. The two simulators are both written in C++ but *ns-3* is a new simulator that does not support the *ns-2* APIs. Some models from *ns-2* have already been ported from *ns-2* to *ns-3*.

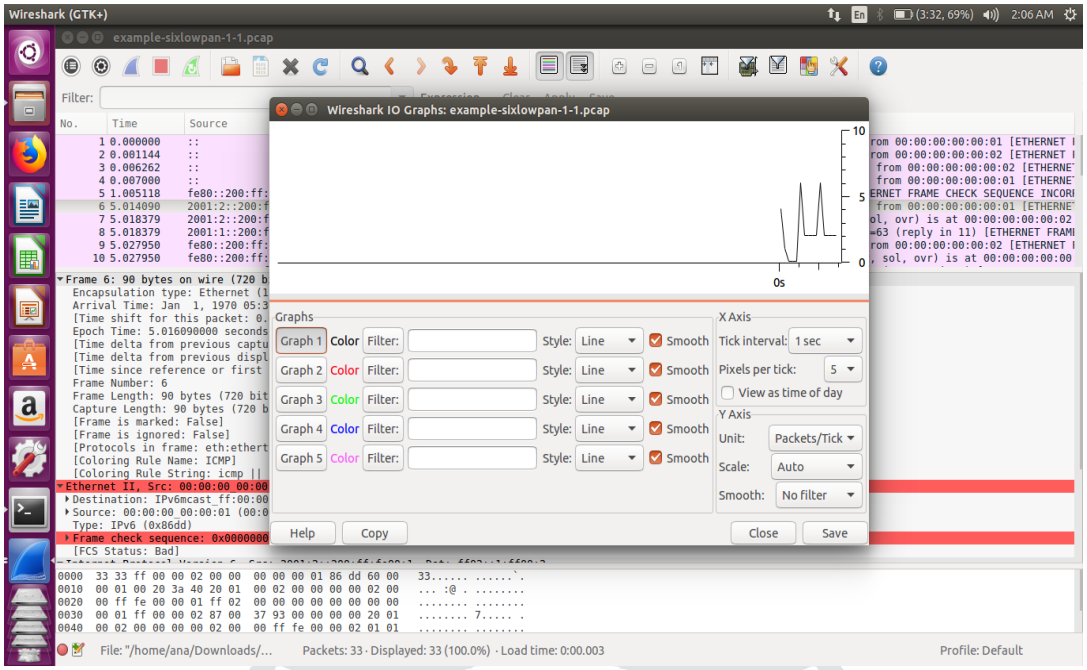
4. RESULTS



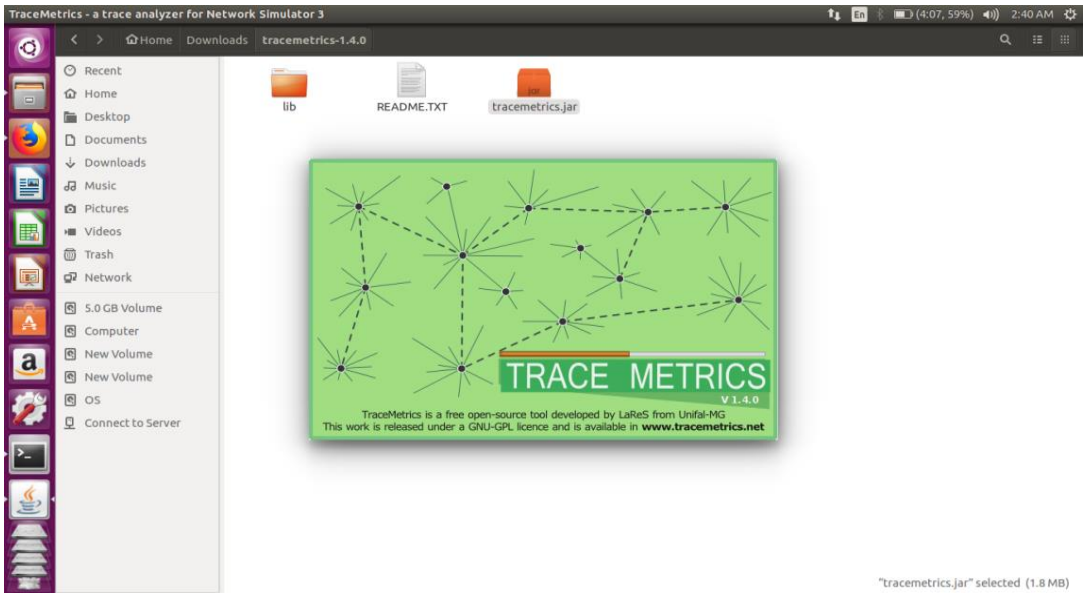
4.1 Nodes Creation



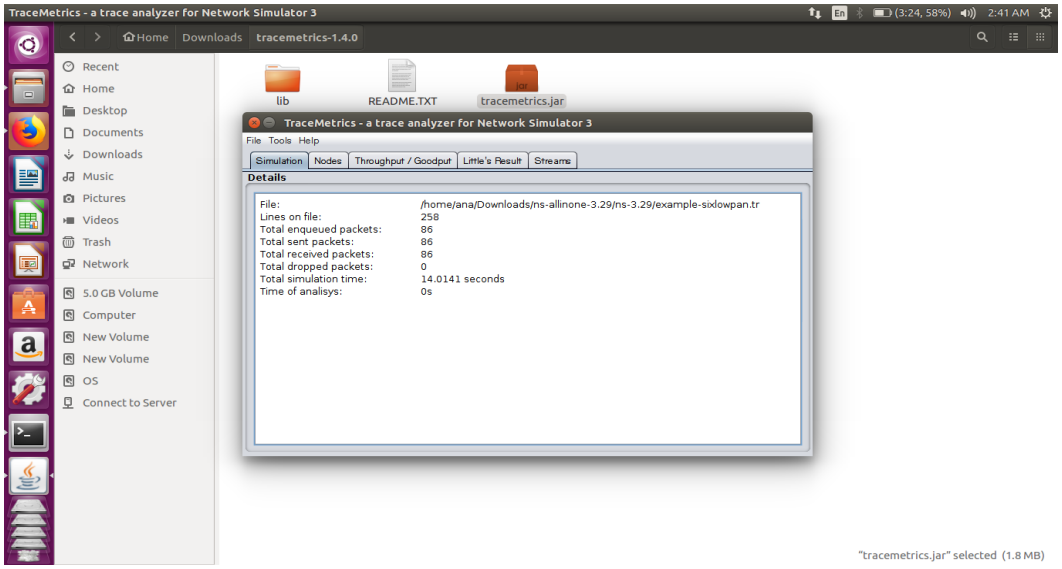
4.2 Packet Analysis Using Wireshark



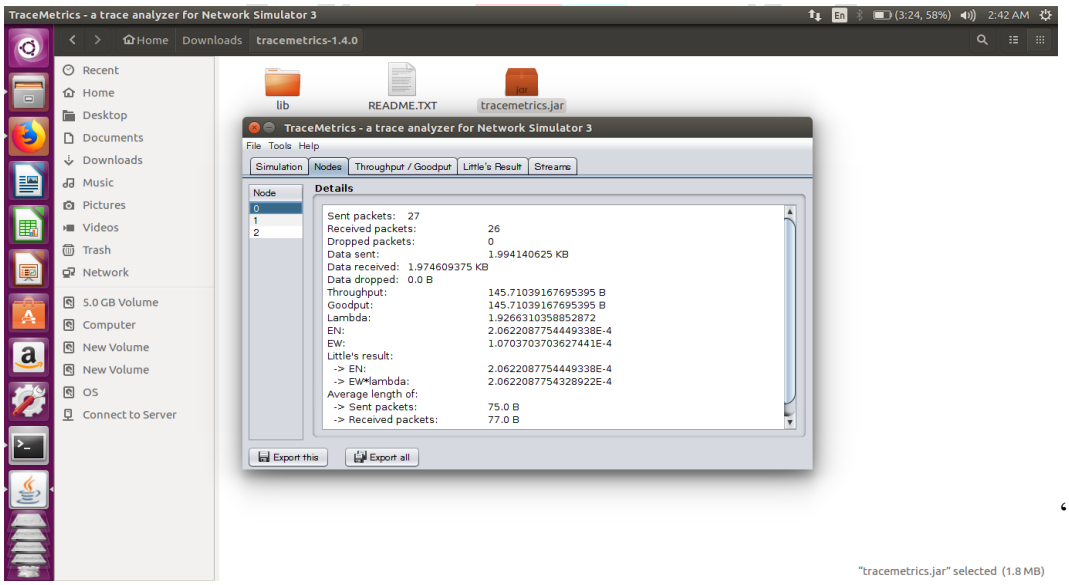
4.3 Graphical representation for packet transformation



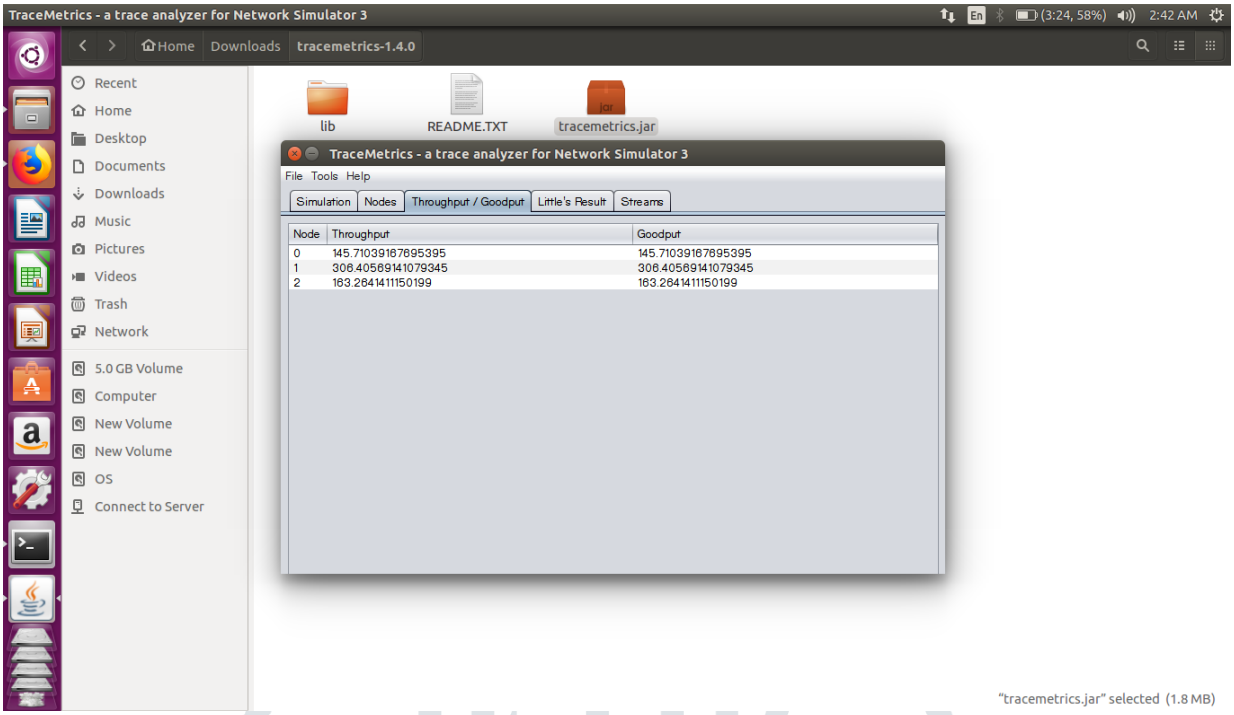
4.4. Splash screen of Tracemetrics



4.5 The Simulation Results



4.6 The Node Wise Statistics



4.7 The throughput & good put

5. CONCLUSION

In this project we simulate the communication in between three nodes i.e IoT devices and the files is analyzed by using Trace matrix (trace file analyzer for Network Simulator-3). We analyze packets using wire shark and the data is saved in encrypted manner using block chain technology. To carry out the project we used the Network Simulator-3, C++ and Python programming languages.

This project can be extended by simulating more than three nodes and packets including data can be analyzed by applying DDOS attack.

References

[1] B. Krebs, "Krebsonsecurity Hit with Record DDoS." https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-recordddos/, 2016. [Accessed 19.5.2017.].

[2] OVH, "The DDos that didn't break the camel's VAC." https://www.ovh.com/us/news/articles/a2367.the-ddos-that-didnt-breakthe-camels-vac, 2016. [Accessed 19.5.2017.].

[3] S. Hilton, "Dyn Analysis Summary Of Friday October 21 Attack." https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21- attack/, 2016. [Accessed 19.5.2017.].

[4] H. Chen and D. Wagner, "Mops: An infrastructure for examining security properties of software," in Proceedings of the 9th ACM Conference on Computer and Communications Security, CCS '02, (New York, NY, USA), pp. 235–244, ACM, 2002.

[5] H. H. Feng, J. T. Giffin, Y. Huang, S. Jha, W. Lee, and B. P. Miller, "Formalizing sensitivity in static analysis for intrusion detection," in IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004, pp. 194–208, May 2004.

[6] H. Chen, D. Dean, and D. Wagner, "Model checking one million lines of c code.," in NDSS, vol. 4, pp. 171–185, 2004.

[7] K. Thompson, "Reflections on trusting trust," Commun. ACM, vol. 27, pp. 761–763, Aug. 1984.

[8] F. B. Cohen, A Short Course on Computer Viruses. New York, NY, USA: John Wiley & Sons, Inc., 2nd ed., 1994.

[9] C. Willems, T. Holz, and F. Freiling, "Toward automated dynamic malware analysis using cwsandbox," IEEE Security Privacy, vol. 5, pp. 32–39, March 2007.

[10] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware-analysis techniques and tools," ACM Comput. Surv., vol. 44, pp. 6:1–6:42, Mar. 2008.

[11] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "Iot security: Ongoing challenges and research opportunities," in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234, Nov 2014.

[12] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, and C. Rossow, "Iotpot: Analysing the rise of iot compromises," in Proceedings of the 9th USENIX Conference on Offensive Technologies, WOOT'15, (Berkeley, CA, USA), pp. 9–9, USENIX Association, 2015.

[13] I. Z. Ben Herzberg, Dima Bekerman, "Breaking Down Mirai: An IoT DDoS Botnet Analysis." https://www.incapsula.com/blog/malwareanalysis-mirai-ddos-botnet.html, 2016. [Accessed 20.5.2017.].

[14] D. Web, "Investigation of linux.mirai trojan family," tech. rep., Doctor Web, 2016.

[15] E. Bertino and N. Islam, "Botnets and internet of things security," Computer, vol. 50, pp. 76–79, Feb 2017.

[16] K. Angrishi, "Turning internet of things(iot) into internet of vulnerabilities (iov) : Iot botnets," CoRR, vol. abs/1702.03681, 2017.

[17] J. v. H. Ivo van der Elzen, "Techniques for detecting compromised iot devices," tech. rep., University of Amsterdam, 2017.