International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 6 114 - 118

Network Forensics for detection of malicious packets in Internet of Things (IoT)

Meet Tilva
GTU PG School, Ahmedabad, India
tilva007@gmail.com

Vandana Rohokale
SKNSITS Lonavala, India
Vmr.301075@gmail.com

Abstract: - In the internet of things there are various devices which are interconnected to the other devices which share different technology and the different standards. The rise of new technology in various fields it also makes rise to the new challenges in the area of the forensic investigation. As there will be many new challenges to the forensic investigators. The recent tools and the process flow carried out will not meet the highly distributed and current infrastructure of the IoT. Forensic researcher will have a lot of challenges to face in collecting the piece of evidence from the infected component in the IoT Environment and also will face complication to analyze those evidence. In this paper, we will do the network forensics on the simulated IoT Environment and we will carry out the forensics investigation in the simulated environment.

Keywords*: Internet of Things, Network Forensics, IoT Forensics, IoT Security, Packet detection, Cooja, Contiki OS.*

*****

1. INTRODUCTION

The advancement of the internet and the innovative development of the smart electronic devices leads to the development of the new computing prototype – The Internet of Things (IoT). IoT is considered the future estimation of the internet which works on the Machine-to-Machine (M2M) communication and the Radio Frequency Identification (RFID) [1]. The main goal of the IoT is to allow the secure exchange of the data between the real world devices and applications.

The Internet of Things has become quite familiar in the recent years. Many of the daily routine devices are getting connected with us that include many capabilities like sensing, autonomy and contextual awareness [6]. IoT devices include personal computers, laptop, Smartphone, tablet, and other home embedded devices [2]. These devices are connected to each other and share a same network for communicating with each other. These all the devices are connected with the sensor to detect the particular surrounding condition and analyze the situation and work accordingly. Devices are also programmed to take the decision automatically or inform according to the user so that the user can make the best decision.

This interconnected network can bring lot of advancement in the technology of application and services that can bring economic benefit to the global business development. Lot of devices are getting connected to the internet to share the local information to the cyberspace. According to the analysis report, there will be approximately 35 billion things connected to internet with the different connectivity media. Since many devices will be connected to the IoT which ultimately turns the attention to the hacker in breaking the security mechanism[2]. To investigate such attacks we need to apply the aspects of the digital forensics in the IoT parameter which is called as IoT Forensics [1].

As the Digital Forensics in the IoT Paradigm is very challenging and diverse, the traditional model of the forensics does not fit with the recent IoT Environment. The large number of the devices will also bring new challenges for the data management. The large number of IoT devices generating large data also makes it difficult for the investigator to analyze the data.

2. BACKGROUND

This section gives the brief explanation of the digital forensics and the Internet of things. Also it will explain in brief the network forensics and present a hypothetical scenario for the digital forensics in the IoT Environment.

A. Digital Forensics.

Digital Forensics is "a branch of science which encompasses the recovery and investigation of material which is found in digital devices, often related to computer crime. In the digital forensics we will first be incorporating on the network forensics.
The Network Forensics is the branch of the digital forensics which deals with the monitoring, capturing, recording, and analysis of the network traffic [7]. "Marcus J Ranum' proposed the term 'Network Forensics' in the early 90's

B. Network Forensics Process Model

In the paper "A survey about network forensics" the author proposed a model of the network forensics investigation. This proposed model consists of many different phases of network forensics investigation. The figure 1 shows the model of network forensics which has nine phases illustrated [7].

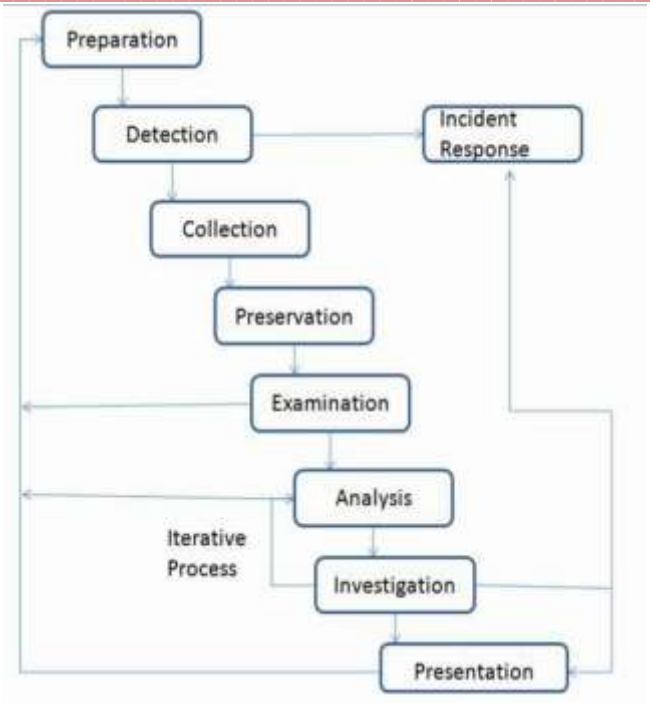

Figure1- Network Forensic Process Model

- **Preparation Phase: -** The main objective is to obtain required authorization and legal warrants.
- **Detection Phase:-** Generate a warning or an alert which indicate security violation.
- **Incident Response Phase:-** Applicable only when investigation is initiated during the attack.
- **Collection Phase:-** The most difficult part because the data flows rapidly and is no possible to generate later traces of the same thing.
- **Preservation Phase: -** Original Evidence is kept safe along with computed hashes.
- **Examination Phase: -** Examines the previous phase. All hidden or altered data is to be uncovered which is done by the attacker.
- **Analysis Phase: -** Collected evidence is analysed to find the source of intrusion.
- **Investigation Phase:** Use information gathered in the analysis phase and focus on finding the attacker.
- **Presentation: -** Final stage for processing the model. Here the documentation is made and the report is generated and is shown to the higher authority.

C. Forensic in IoT Environment

The IoT Forensics is also one of the specialized branch in the digital forensics where all the phases discussed deals with the IOT infrastructure to find facts about the crime happened in IoT environment. The IoT Forensics is carried out in the three levels of forensics Cloud level forensics, network level forensics, device level forensics this can be explained in the Figure 2[9].

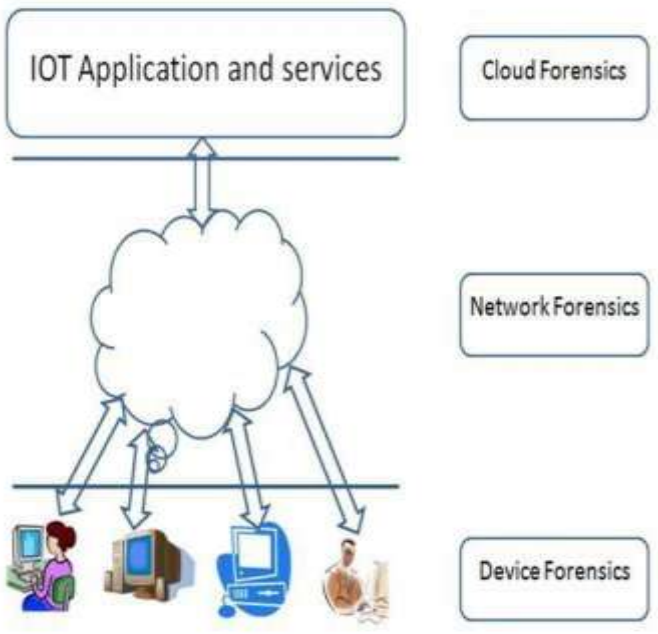

Figure 2 - IoT Forensics

- **Device level Forensics:** Here in this level the investigator has to collect the small piece of evidence from the devices which work on the IOT. The infected devices are identified and reported.

- **Network level Forensics:** In this level the different attacks are identified through the network logs and malicious packet detection across different networks this can be local area network (LAN), Wide Area Network (WAN).

- **Cloud Forensics:** It is one of the most important part in the IOT because all of the data generated from the IOT devices and IOT networks are stored in the cloud. As the cloud offers many features such as large storage and infrastructure there will be much scope.

3. STATE OF ART

We seen that how the IOT Forensics environment works and the three level of forensics needs to be carried out in the IoT scenario to find out the actual source of the infected device or the network breach[5]. Here in this section we will do the comparison of the different parameters how the how the actual system works and how the proposed solution is to be carried out [3].

Parameters	Traditional and IOT Forensics Comparison	
	Traditional Forensics	IOT Forensics
Evidence	Computers, cloud, devices, servers, gateways, mobile devices	Home appliances, car tags, readers, embedded system, nodes,
Devices connected	Billions of Devices connected	50 billions devices connected by 2020 according to Gartner.
Networks	Wired, wireless, Bluetooth wireless network, internet	RIFD, Sensor Network
Protocols	Ethernet wireless (802.11 a,b,g,n), Bluetooth, Ipv4 and Ipv6	RFID, Rime
Size of the digital Evidence	Up to Terabytes of data	Up to Exabyte of data

Table1-Comparison of Traditional and IoT Forensics

4. CHALLENGES

The traditional tools and technologies are not designed completely to carry out forensic in the IOT environment as it faces many challenges [8]. In this section we will identify the challenges we are facing for the forensic investigation in IoT environment [1].

I. Compromised device identification in IoT.

the criminal. For e.g., there are number of devices in the college and if any of the devices gets compromised and gets breach on the network and extract some of the personal files it will be very hard to find the source of the device which got infected. This challenge is like finding the needle in the haystack.

II. Gathering and analysis of data.

After identification there comes the analysis and gathering which is quite a challenging task to find the piece of evidence [7]. This phase is very crucial phase and depends on the other phase also resulting the error to other phase.

III. Data Organization

The wide variety of data generated by the IoT devices makes the collection and analysis phase challenging. The proper logs need to be organized in order to avoid the complication of the data and files.

IV. Preservation of Evidence.

The final step of the forensic investigation is that the forensic examiner presents the gathered information and the evidence in front of the court of law. As in comparison traditional forensic evidence presentation is easy than the forensic of the IoT Environment as it is challenging task as the jury members don't have enough knowledge as compared to the technical person. They also feel complex to understand

5. Proposed Method

1) Network Forensics for malicious packet detection.

Since we know that the IoT forensics comprises of three different level of the forensics to be carried Cloud Forensics on the cloud environment, Device Level Forensics on the device inspection, Network Forensics on the network for analyzing and recording the traffic[1]

The number of IoT devices will generate a huge in the data. Here we will do the network amount of the data. As the amount of data evidence will be very large and will be very hard to analyze those data and difficult to identify the piece of evidence which can be used to identify forensics for finding the malicious packets and by monitoring that we will be able to identify the source of that attack which device was infected.

The network consists of the packets that flow through the signal over the network. A packet also includes the control information and the user data, which is also known as payload. Control information provides information for delivering the payload i.e. the source and destination network address. They control the header and trailer information of the packets.

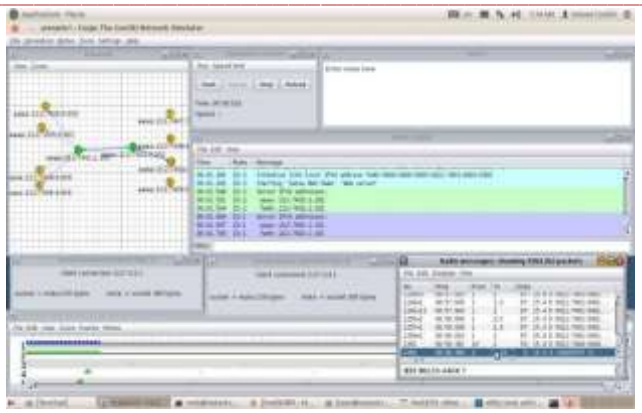

Figure3- Communication and monitoring of packets in Contiki Cooja Simulator

For the development of the IoT Environment, we will be doing with the help of the Contiki os [10]. Cooja is the Contiki network simulator. Cooja allows large and small networks of Contiki motes to be simulated. Motes can be emulated at the hardware level, which is slower but allows precise inspection of the system behavior, or at a less detailed level, which is faster and allows simulation of larger networks [12][10].

The motes in the Contiki are nothing but the devices which are connected to the environment, and these motes need a communication between the devices which is done by the wireless sensor nodes for the establishment of the communication [11].

For the deployment of the complete local and home network, the motes are deployed in the simulator.

After deploying the motes, the communication in the particular network does not start the motes need a communication medium to communicate with the outer environment so that the border router needs to be set up. The border router technically acts as a gateway for the particular network and communicates with the internet. The border router can only be activated by the starting of the tunslip protocol. In order as we are communicating with the ipv6 standard in this simulator so that the tunslip6 protocol is used in this which can be started from the terminal. After activating the tunslip6 we can now connect the border router with the motes, and it will be connected to the local network, and we will be able to communicate with the border router. We can now be able to communicate with the two border router as shown in the figure. How the two different network communicates with each other sharing the same network.

Shown in the figure we can see that how the two different local network communicating with each other the mote 1 is communicating with the mote ten which is on the other zone that's how the process of communication between the different networks work in the Internet of Things. There is mote output console which monitors the operation of the motes. The next is the socket server of the motes of the border router which is connected to the network [13]. The next box is the radio messages box which monitors the radio packets that what packets are sent to the other motes and which motes are communicating with whom are clearly seen and tracked here[14].

If the attacker wants to attack in the particular environment the attacker will suppose do the attack to the particular system the denial of service attack and suppose the attacker does the attack the particular machine of the user which will be in the particular area will be compromised and incase the data will also be destroyed. The dos attack in the ipv6 platform will be demonstrated here that how it affects the system and the performance and the system may crash at that time also.

To investigate where the attack was generated the system. We will use the log analysis method to identify that what kind of attack was generated and from where the attack was generated. This is the toughest phase to do the log analysis that where the attack was generated and to find the attack source location. Once the attack location of the attacker is found out the attack can be traced and can be found out.

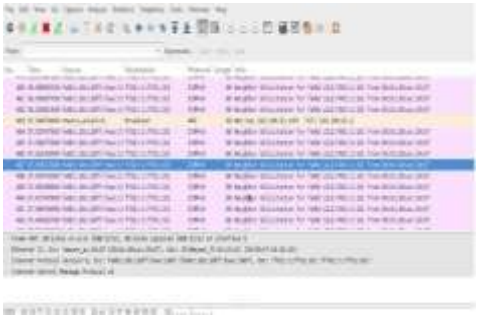

Figure-4 Denial of service attack performed in the IoT Environment.

We can see the how the Denial of Service (DoS) attack is performed in the IoT environment in the ipv6 platform. Here the attacker from the different location has performed the attack in another environment in the IoT. So the user is unaware about it and when he sees and identifies the user knows that the user's pc has been compromised and he calls the forensics investigator to investigate the pc and to determine the source of the attack.

The forensic investigator starts from the beginning for the investigation and the investigator investigates the whole machine which has been compromised. Here the user does the log analysis for finding the traces of the packets where the attack has been originated and he scans the whole network and he comes to know that the denial of service attack is performed in the system. He searches the whole network find that it came from the outside network.

He then scans the whole network and analyze the logs whether the log came from that network or not. To analyze the whole different network and the logs is very difficult task and it is time challenging. Finally the user finds the traces and he comes to know the zone where the particular attack was generated.

The user then analyze that whole particular network here in this case there will be many devices connected to identify that logs are analyzed and ultimately the user finds the particular device where the device was compromised and then he does the countermeasures on that particular device.

6. CONCLUSIONS AND FUTURE SCOPE

The rapid infrastructures increase in the growth of IoT so that the security of the IoT should also be given the highest priority. With the new advancement in the devices it also gives new challenges in the forensic investigation. In this article we proposed the method to carry out the forensic investigation and to trace the source using the network forensics for detection of the malicious packets in the infected device. In this paper, the authors have presented the network forensic model for detecting the packets and identifying the source of the packets. Here further we are going to detect the malicious packets and will find the source infected device. This work can even more be extended to make the network forensic investigation even more secure with a log based mechanism to make the system more secure and it becomes easy to find the particular defects of the system.

REFERENCES

[1] Zawoad, Shams, and Ragib Hasan. "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things." *Services Computing (SCC), 2015 IEEE International Conference on*. IEEE, 2015.

[2] Hossain, Md Mahmud, Maziar Fotouhi, and Ragib Hasan. "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things." *Services (SERVICES), 2015 IEEE World Congress on*. IEEE, 2015.

[3] Oriwoh, Edewede, et al. "Internet of Things Forensics: Challenges and approaches." *Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), 2013 9th International Conference Conference on*. IEEE, 2013.

[4] Oriwoh, Edewede, and Paul Sant. "The Forensics Edge Management System: A Concept and Design." *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*. IEEE, 2013.

[5] Karyda, Maria, and Lilian Mitrou. "Internet forensics: Legal and technical issues." *null*. IEEE, 2007

[6] Bandyopadhyay, Debasis, and Jaydip Sen. "Internet of things: Applications and challenges in technology and standardization." *Wireless Personal Communications* 58.1 (2011): 49-69.

[7] Almulhem, Ahmad. "Network forensics: Notions and challenges." *Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on*. IEEE, 2009

[8] Buric, J., and D. Delija. "Challenges in Network forensics." *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2015 38th International Convention on*. IEEE, 2015.

[9] Perumal, Sundresan, Norita Md Norwawi, and Valliappan Raman. "Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology." *Digital Information Processing and Communications (ICDIPC), 2015 Fifth International Conference on*. IEEE, 2015.

[10] Paul, Tomsy, and G. Santhosh Kumar. "Safe contiki os: Type and memory safety for contiki os." *Advances in Recent Technologies in Communication and Computing, 2009. ARTCom'09. International Conference on*. IEEE, 2009.

[11] Muthanna, Ammar, et al. "Comparison of protocols for Ubiquitous wireless sensor network." *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2014 6th International Congress on*. IEEE, 2014.

[12] Osterlind, Fredrik, et al. "Cross-level sensor network simulation with cooja." *Local computer networks, proceedings 2006 31st IEEE conference on*. IEEE, 2006.

[13] Akshay, Naregalkar, et al. "An efficient approach for sensor deployments in wireless sensor network." *Emerging Trends in Robotics and Communication Technologies (INTERACT), 2010 International Conference on*. IEEE, 2010.

[14] Le, Quan, Thu Ngo-Quynh, and Thomaz Magedanz. "RPL-based multipath Routing Protocols for Internet of Things on Wireless Sensor Networks." *Advanced Technologies for Communications (ATC), 2014 International Conference on*. IEEE, 2014.