Detection of Intruders in IOT Networks Using Interloper Software based on Authentication

Ch Mohan Kumar, T Rahul Ratna, S Geethika, S Uday Kiran

Abstract**:** ***Present day, we are using different types of IOT devices say both wired and wireless. In this paper we mainly concentrate on wireless devices which will be connected in a network, we call it internet. This phenomenon is nothing but internet of things. There are vulnerabilities for networks and the devices which can be compromised by using attacks. These vulnerabilities has raised the importance for the data protection. This situation is to be dealt with Intrusion detection system. So we need an IDS to check for the authentication and maintaining security of the data. IDS acts as a bridge between the IOT devices and Internet. This IDS comprises of a device along with a software to check for authentication. Final goal of this paper is to achieve a secured IOT network. Identification and Authentication play an important role in this process.***

Index Terms**:** ***IOT, ARP Spoofing, MITM attack, Fog Computing, DNS, IOT Attacks, and IOT Protocols.***

I. INTRODUCTION

IOT is a network where different applications devices like home appliances (Refrigerator, Micro ovens, TVs etc.) are connected to one another. In IOT network, objects interact with the sensors which make them smart. These smart things or objects use eccentric addressing to communicate with each other in the network. In this case we need to make sure that the information in the network maintains confidentiality, reliability and integrity. IDS plays a key role in these security aspects.

There are many attacks say Man-in-the-Middle (MIM) which leads to loss of data. ARP Spoofing is also one of the techniques to hack into the network. In this paper we are going to discuss about such attacks and their casualties. Moreover we will also see some solutions to prevent difficult times. The following fig.1 is the block diagram of IDS in an IOT network.

Revised Manuscript Received on April 07, 2019.

Ch Mohan Kumar, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh 522502, India

T Rahul Ratna, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh 522502, India

S Geethika, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh 522502, India

S Uday Kiran, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh 522502, India

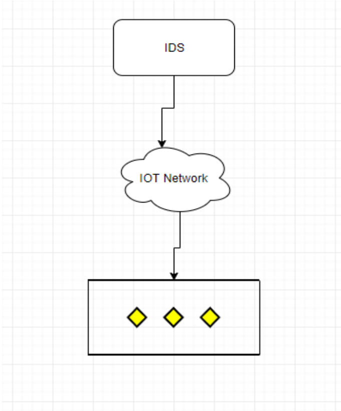


Fig 1.Block diagram

II. Related Concepts

A. IDS Communication Architecture

It uses a five layered architecture. There are different layers in each Architecture. Each layer has its own importance. The diagrams of two architectures are given below.

Application layer and perception layer are also present in 5 layered architecture [12].

5 Layered Architecture

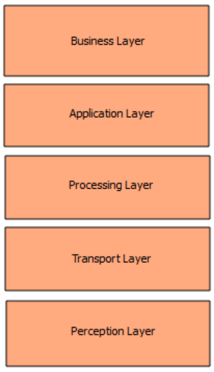


Fig 2.Communication Architecture

Knowing the uses of each layer is very important [2], because each layer has its own significant role in communication.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

1) Application Layer: This layer helps in knowing the protocols that are used by the hosts in the communication and the interface methods used depending on the type of application.

2) Business Layer: This layer is going to be in such a way that it should support the application in a certain way depending on user profiles and business profits.

3) Processing Layer: This layer handles all the processing works like storage, analysis of data. Moreover it is able to handle huge amount of data at a time. It is also known as middle-ware layer.

4) Transport Layer: End to End communications are held by this layer means ports required in communication are specified this layer [17].Each protocol requires a significant port.

5) Network Layer: This layer includes Logical addresses (IP) which is used to locate a host. Data is converted into packets before transmission. Moreover routing path for the packets is managed by this layer [18].

6) Physical Layer or Perception Layer: The name itself says that it does physical work like converting data into signals in case of wireless networks (or) transmission through Wires and cables in case of wired networks [19].More over sensing the signals in case of sensors.

B. MAC

Medium Access Control transmits the data through physical layer [3].It converts the data into frames before transmission. It provides collision avoidance by CSMA/CA, a protocol which helps in sensing the channel to know whether it is idle or not. If idle then transmit else wait for it to be idle by this we achieve collision avoidance. So that loss of data can be brought down. Specifically speaking about MAC 802.15.4 tells us about the LR-WPANS (low rate wireless PANS).Moreover MAC layer also involves finding and verifying the MAC address which plays a crucial role in this paper.

C. IOT Protocols Mechanism used by IDS

Communication takes place in 2 steps using protocol [4].

1) Requestor, a host initiates the communication by sending a request message to the other host.

2) Responder, one who sends a response message back to the host who sent the request.

Many IOT protocols use the same process say MQTT, Message queuing telemetry protocol uses this mechanism which is the basic prerequisite knowledge required to be known.

D. Identification

Identification in a network means that we should be able to detect whenever a host/device enters a network. This identification is done sometimes based on digital certificates which contain digital signatures [9].These are accessed with public and private keys exchanged during session between any of the hosts. Further step of identification is authentication which should be performed strictly.

E. Authentication

Authentication means one who is going to enter into a network should be checked whether is he entering with true details and moreover not violating any policies (For real world example: It's like checking while entering into a movie theatre) [13].We need to maintain authentication for a network else we could not know who is coming and going in the network. In the IOT scenario this is tough job due to the way of working and the framework of the devices. In normal communication devices there is lot of advancement on this topic but not in the case of IOT.

Every network should maintain authentication or else that network and the hosts of the network may get attacked. Some of the attacks are given below which are used by attackers in IOT domain.

F. Attacks

1) **Man in the middle attack:** The Name itself says when there is transfer of packets between hosts in a network. An attack can be able to capture the packets in between and manipulate the packet without leaving any trace of his presence. This manipulation leads to loss of confidentiality and sometimes leads to loss of integrity. The entire session is controlled by the attacker [5].

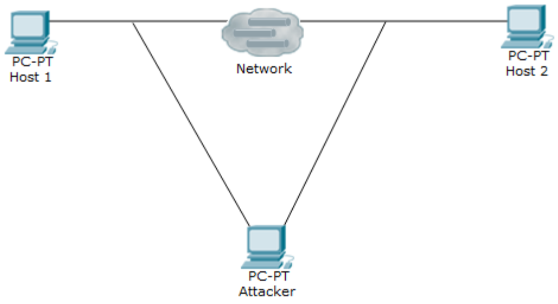


Fig 3.MITM attack

2) **Botnets:** Many systems connected in a network comprises a Botnet [11].These botnets are used to spread malwares or viruses across. Also taking control over the servers and devices using command interface. These are used by criminals in hacking the bank servers to take control over their network.

3) **Social Engineering:** This is one interesting attack in which people are made to give up their information [6]. This attack involves phishing sites and also redirections to a webpage which looks like a trusted one asking for personal info. There are different types of attacks in DOS, Denial of Service.

4) **Node Replication Attacks:** In this attack, a new node or a hub which should act as an access point will be replaced or manipulated by attacker in order to gain control over the network and also in creating new packets. This also leads to degradation in performance of network [10].

5) **Physical Attack:** The attacker is able to get access to the physical device. So that he could easily detect the cryptography and decode it. Moreover working of device is changed to his appropriate way.

G. ARP Spoofing

Any host who wants to connect to a network has to go with a Request and Response protocol [7]. So while doing so, if there is an attacker who starts to analyze packets in the local area network by entering in to the network using protocols. An attacker can manipulate his IP address but not the MAC address it remains untouched.MAC address is also used for communication. The Request packets that are sent to the network by the host will be rerouted to the host with response packets. The attacker starts to capture the packets of the host, then he is able to attack the host to manipulate his data by knowing all about the host.

H. MAC based Interloper

Interloper is a software which was written in python. This is monitoring software which is capable to identify all hosts who are in the network and also those who are entering into the network. It identifies hosts by knowing their MAC address and IP address.

I. Fog computing system

Fog computing, which is also known as edge computing is a decentralized form of a network in which processing of the data happens in the lower level nodes of the network where the data is stored and updated [8].By using this we could reduce the load on the central server and network becomes more efficient. This is related to cloud computing where the data is transferred to far away for processing which may lead to loss of confidentiality, integrity etc. Our Interloper software is similar to this fog computing since it is implemented in the lower level nodes. We are able to detect the intruder at the early stages itself which is more profitable in the current scenario.

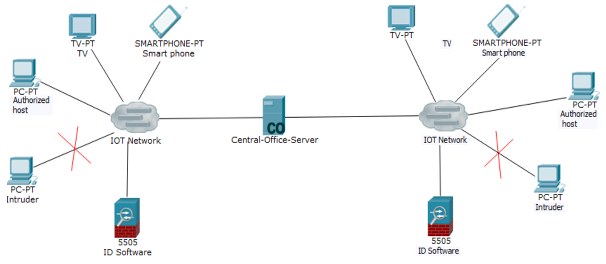


Fig 4.IDS using FOG Computing

III. Working of Interloper Software

This software is able to detect the intruders in a network who are trying to manipulate the data by capturing the packets [20].This could be done with man in the middle concept. Whoever enters into a network has to go with request-response packet mechanism. While doing so the attacker enters the network with a different IP which is not the original one. Even then when he enters this software will analyze the packets sent by the intruder and finds his IP and MAC addresses. The found IP may not be true but the MAC address found is the original MAC address of the intruder. These addresses are logged into a log file along with the time stamp. So whenever there is malicious activity found in the network we are ready to trace the attacker as we have his MAC address logged with us.

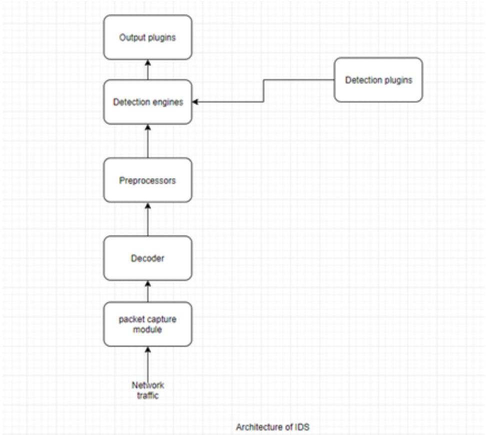


Fig 5.Working architecture of IDS

IV. Interaction between the Interloper and IOT Things

This is the software which is used to log the IP addresses and MAC addresses of hosts or devices on the network. This software uses the Request-Response mechanism packets to trace the IP and MAC addresses using pyshark and the scapy libraries of Python. This software is kept running as a process in order to detect those who newly enters into the network.

IP Addresses	MAC Addresses
192.168.0.1	e8:94:f6:f8:2e:a0
192.168.0.101	10:07:b6:ac:2b:38
192.168.0.103	bc:d1:1f:f6:7a:47

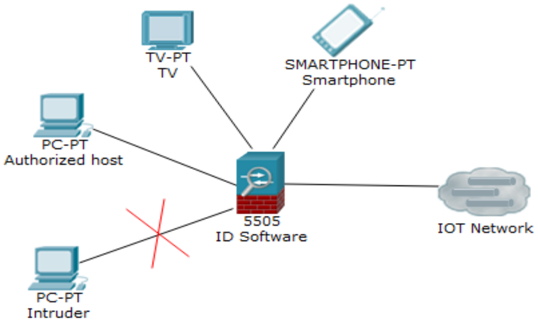
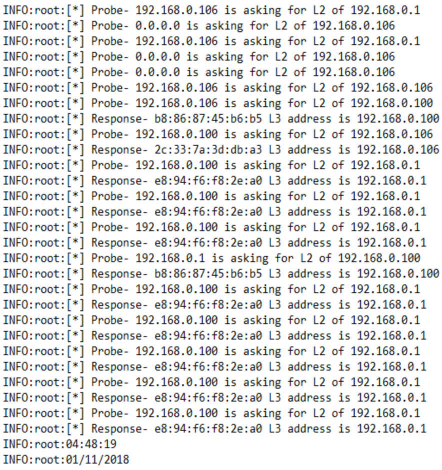


Fig 6.Interaction with IOT things

V. Experiment Observation and Results

This Interlope Software is tested on various networks including IOT. We also acted as a virtual attacker (With different IP) to the network where the Software is able to detect the attacker's MAC address. The results of the test are followed. The Table shows the Hosts or devices IPs and MAC addresses. This data is obtained as and when the program is executed present devices in the network at the time of execution. As these are the devices that are connected in the network at that time, but we need to keep analysing for new connections so following results tell about the new connections scenario.



```
INFO:root:[*] Probe- 192.168.0.106 is asking for L2 of 192.168.0.1
INFO:root:[*] Probe- 0.0.0.0 is asking for L2 of 192.168.0.106
INFO:root:[*] Probe- 192.168.0.106 is asking for L2 of 192.168.0.1
INFO:root:[*] Probe- 0.0.0.0 is asking for L2 of 192.168.0.106
INFO:root:[*] Probe- 0.0.0.0 is asking for L2 of 192.168.0.106
INFO:root:[*] Probe- 192.168.0.106 is asking for L2 of 192.168.0.106
INFO:root:[*] Probe- 192.168.0.106 is asking for L2 of 192.168.0.100
INFO:root:[*] Response- b8:86:87:45:b6:b5 L3 address is 192.168.0.100
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.106
INFO:root:[*] Response- 2c:33:7a:3d:db:a3 L3 address is 192.168.0.106
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.1 is asking for L2 of 192.168.0.100
INFO:root:[*] Response- b8:86:87:45:b6:b5 L3 address is 192.168.0.100
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:[*] Probe- 192.168.0.100 is asking for L2 of 192.168.0.1
INFO:root:[*] Response- e8:94:f6:f8:2e:a0 L3 address is 192.168.0.1
INFO:root:04:48:19
INFO:root:01/11/2018
```

In the above results 192.168.0.106 is an attacker as he joined into the network with a VPN which should hide his IP address only but not the MAC address. You can see that the attackers MAC address is resolved and logged. These results are maintained in log files. All this work is done at the initial level of the network.

VI. Conclusion and Future Work

Future of this project is to improve the software in such a way that we are able obtain more secured IOT network and moreover it is able to detect many other attacks and injections. Also trying to trace out the original IPs of the attackers. And implementing this software on various networks i.e. networks containing devices with different bandwidths. Moreover this process has to be done in an optimal and efficient way.

References

1. Singh, Dhananjay, Gaurav Tripathi, and Antonio Jara. Secure layers based architecture for Internet of Things. Internet of Things (WF-IoT), 2015 IEEE 2nd World Forum on. IEEE, 2015.
2. Mustika, I. Wayan. Implementation of Digital Signage Based on Embedded System and IoT Using Mac Address as an Identifier on Laboratory in-Out Announcer Board. 2018 4th International Conference on Science and Technology (ICST). IEEE, 2018.
3. Sharma, Cheena, and Naveen Kumar Gondhi. Communication Protocol Stack for Constrained IoT Systems. 2018 3rd International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). IEEE, 2018.
4. Okul, Ş., and M. Ali Aydın. Security Attacks on IoT. Computer Science and Engineering (UBMK), 2017 International Conference on. IEEE, 2017.
5. Deogirikar, Jyoti, and Amarsinh Vidhate. Security attacks in IoT: a survey. I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on. IEEE, 2017.
6. Al-Shaboti, Mohammed, et al. "Towards Secure Smart Home IoT: Manufacturer and User Network Access Control Framework." 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA). IEEE, 2018.
7. Zhang, Guowei, et al. "FEMTO: Fair and Energy-Minimized Task Offloading for Fog-Enabled IoT Networks." IEEE Internet of Things Journal (2018).
8. Alizai, Zahoor Ahmed, Noquia Fatima Tareen, and Iqra Jadoon. Improved IoT Device Authentication Scheme Using Device Capability and Digital Signatures. 2018 International Conference on Applied and Engineering Mathematics (ICAEM). IEEE, 2018.
9. Umrao, Sachin, Deeksha Verma, and Arun Kumar Tripathi. Detection and Mitigation of node Replication with pulse delay attacks in wireless sensor network. Innovation and Technology in Education (MITE), 2013 IEEE International Conference in MOOC. IEEE, 2013.
10. Nguyen, Huy-Trung, Quoc-Dung Ngo, and Van-Hoang Le. IoT Botnet Detection Approach Based on PSI graph and DGCNN classifier. 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP). IEEE, 2018.
11. Liao, Lijun, et al. Layered Semantic Analysis of Software Architecture. Intelligent System Design and Engineering Application (ISDEA), 2012 Second International Conference on. IEEE, 2012.
12. El-hajj, Mohammed, et al. Analysis of authentication techniques in Internet of Things (IoT). Cyber Security in Networking Conference (CSNet), 2017 1st. IEEE, 2017.
13. Alqinsi, Padlan, et al. IoT-Based UPS Monitoring System Using MQTT Protocols. 2018 4th International Conference on Wireless and Telematics (ICWT). IEEE, 2018.
14. Swamy, Sowmya Nagasimha, Dipti Jadhav, and Nikita Kulkarni. Security threats in the application layer in IOT applications. I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2017 International Conference on. IEEE, 2017.
15. Xiaocong, Qian, and Zhang Jidong. Study on the structure of Internet of Things (IOT) business operation support platform. Communication Technology (ICCT), 2010 12th IEEE International Conference on. IEEE, 2010.
16. Muñoz, Raul, et al. IoT-aware multi-layer transport SDN and cloud architecture for traffic congestion avoidance through dynamic distribution of IoT analytics. Optical Communication (ECOC), 2017 European Conference on. IEEE, 2017.
17. Divarcı, Sinan, and Oguzhan Urhan. Secure gateway for network layer safety in IoT systems. 2018 26th Signal Processing and Communications Applications Conference (SIU). IEEE, 2018.
18. Kumar, Sudeendra, et al. Security Enhancements to System on Chip Devices for IoT Perception Layer. Nanoelectronic and Information Systems (iNIS), 2017 IEEE International Symposium on. IEEE, 2017.
19. Muthanna, Ammar, et al. Software development for the centralized management of IoT-devices in the "smart home" systems. Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian. IEEE, 2017.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

AUTHORS PROFILE

Ch. Mohan Kumar, Assistant Professor Department of CSE KLEF, Guntur, Andhra Pradesh, India.

T Rahul Ratna, a B. Tech (CSE) Student at KLEF, Guntur, Andhra Pradesh, India.

S Geethika a B. Tech (CSE) student at KLEF, Guntur,, Andhra Pradesh, India.

.

S Uday Kiran a B. Tech (CSE) Student at KLEF, Guntur, Andhra Pradesh, India.