

Intrusion Detection and Prevention in Internet of Things

Mr. Maulik Bhensdadia¹ Mr. Aditya Kumar Sinha² Mr. Gardas Naresh Kumar³

¹ Research Scholar

¹Gujarat Technological University, Ahmedabad ^{2,3}CDAC ACTS, Pune

Abstract— Internet of Things is an interconnected system where physical things get to be computerized objects with the ability of correspondence by means of web. The security and protection are a portion of the real issues that keep the wide appropriation of Internet of Things. There are excessively numerous assaults every day happening in Internet of things or by utilizing the Internet on things organize. So there is a less security in IoT. By such a substantial scale use of IoT, it gets to be key and essential to secure the system, keep it from undesirable assault. IoT is as yet developing, yet there are certain issues identified with security like secrecy, uprightness, and accessibility. Here we are attempting to execute the recognition and counteractive action framework in IoT. Propose model is for enhancing the security to identify and keep the conceivable assault on Internet of Things.

Key words: Challenges in IoT network IoT, Intrusion Detection and Intrusion Prevention

I. INTRODUCTION

Recent advances in wireless technology for communication and computing leads to fully automated system in people's day-to-day life, and for this kind of automation system emerging technology is Internet of Things. Through IoT we can extend Information Technology (IT) for our lives. IoT transforming current isolated network and infrastructure into a global network of interconnected objects.

IoT means the interconnecting device with their unique identity in the internet. IoT working on different protocols, standards and mediums with layering approach. IoT includes devices with various sensing, measuring and data capture ability with that achieve identification, location, monitoring and management of interconnected devices [3].

II. INTERNET OF THINGS

The Internet of Things (IoT). IoT is considered the future estimation of the internet which works on the Machine-to-Machine (M2M) communication. The main goal of the IoT is to allow the secure exchange of the data between the real world devices and applications [7].

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. IoT devices include personal computers, laptop, Smartphone, tablet, and other home embedded devices. 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 [4].

The Internet of Things (IoT) is a network of globally identifiable physical objects (or things), their integration with the Internet, and their representation in the virtual or digital world. In order to build the IoT, a wide range of technologies are involved [5].

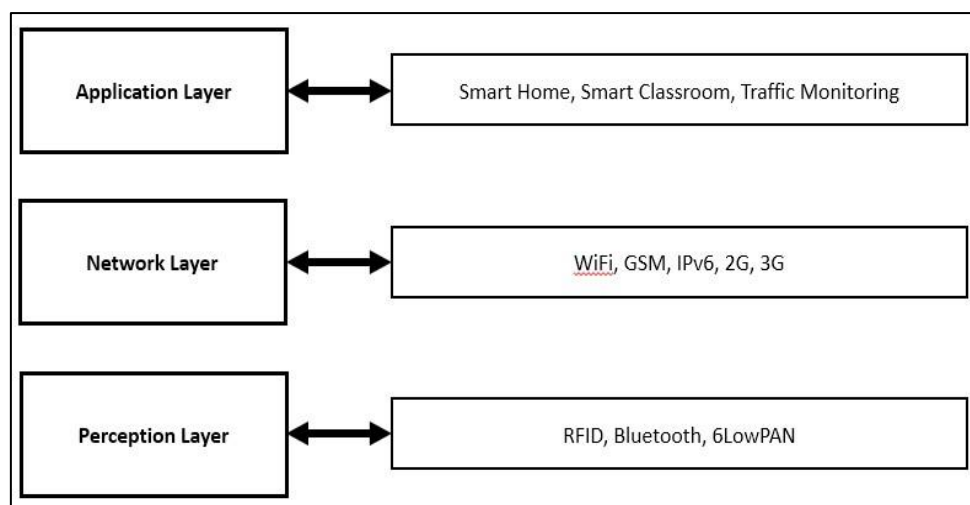


Fig. 1: IOT Architecture

III. INTERNET THREATS

A. Virus

Virus is a small program when it execute its affect other computer by replicate or reproducing itself.

B. Botnet

Botnet is number of computers (Systems) without owner's permission. Botnet is mainly used for DDoS (Distributed Denial of Services) attacks.

C. Malware

Malware is a "Malicious Software"- computer program (software) designed for damage the systems without user known.

D. DoS

DoS (Denial of Service) is an attack for to stop the using services from the user.

IV. INTRUSION DETECTION AND PREVENTION

A. Intrusion

In simple terms, Intrusion is nothing but unauthorized access to network or computer

B. Intrusion Detection

Intrusion Detection is a process to identifying against response of malicious activities targeted at computing device and network resources [6].

Intrusion detection is a process for the detecting a malicious activities in a network and with the detection gives some alerts for it. Intrusion Detection is used for the monitoring the system and finding about the unauthorized access which are getting from the violation of the security policy, system use policy, or any other security standards [2].

Intrusion prevention is a technique used for the prevention against the unauthorized access which is detect through the intrusion detection [2].

To better protection of the system from any kind of attacks, Intrusion Detection and Prevention System (IDPS) is efficiently works. This IDPS system provides a completely automated monitoring services and it is deployed on the systems [2].

V. TYPES OF IDS

A. Host Based Intrusion Detection System

A host-based intrusion detection system (HIDS) is a system that "monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responding through logging activity and with notifying the designated authority". A HIDS can be thought of as an agent that monitors and analyzes the system security whether it is broken or not whether through any kind of internal or external factors through anything or anyone.

B. Network Based Intrusion Detection System

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS observe" all inbound packets and searches for any predefined patterns". When threats are discovered, based on "its severity", the system can take action such as notifying administrators, or restrict the source IP address from accessing the network.

VI. DETECTION TYPES

A. Signature Based

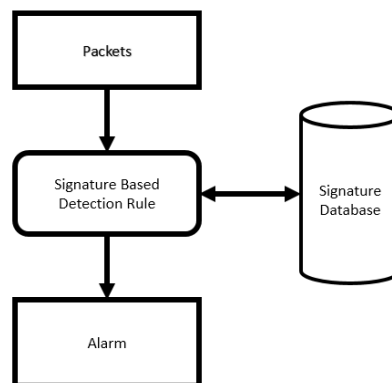


Fig. 2: Signature Based IDS

Signature-based systems are extremely effective against attack which has been detected in the past. They can be installed quickly and become affected immediately. These systems examine each incoming packet and compare its contents against a list of known attack mechanisms. False positives, legitimate activity that appears to be an attack, are rare. Generates the report through this system is easy to understandable in terms of identifying the detected attacks [1].

B. Anomaly Based

Anomaly-based detection system is "detect network activity that does not fit the pattern of expected behavior". The system must be configured, according to "the product with their information on normal patterns of activity". For example, applications may authorize access a single database record at a time. If the intrusion protection system detects access to a "large number of records", the cause is likely to be an attack. Similarly, if a user with permission to access a restricted set of records begins to attempt access to other types of information, the user's workstation is likely to have been infected [1].

VII. CHALLENGES IN IOT

A. Group Membership and Security

End-to-End security of IoT is more important, in this group key is an important security service for IoT. Local broadcast and Multi broadcast relies on symmetric key exchange.

B. Small Devices have Limited Access

IoT devices have low power to run processes. It is difficult to manage the process from low power.

C. Scalable Network

IoT network is able to expand without regulation. In IoT all data shared is contain personal and sensitive information. Our security infrastructure is ready to handle large scalable network.

VIII. ATTACKS IN IOT

There are various types of attacks from both sides in IoT. Internal Attack and External Attack. Attacks are classified in inside and outside. Outside means attacker is not a part of our network. Following we discuss about some attacks on IoT.

A. Sinkhole Attack

In this attack malicious node is attract towards node to shows that this is a shortest path to travel. Attacker activates this type of attack by introducing false node in the network.

B. Selective Forward Attack

In this attack attacker creates malicious node and this malicious node act like a normal node but it drop some selective packets.

C. Sybil Attack

Malicious node has multiple identification.

IX. PROPOSED SOLUTION

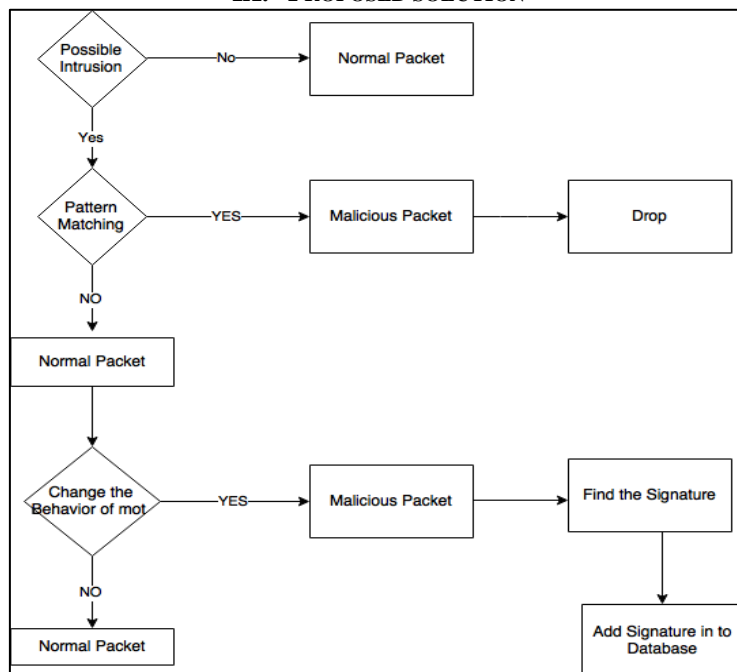


Fig. 3: Flow of proposed solution for attack detection

X. PROPOSED WORK

A. Wormhole Attack Detected

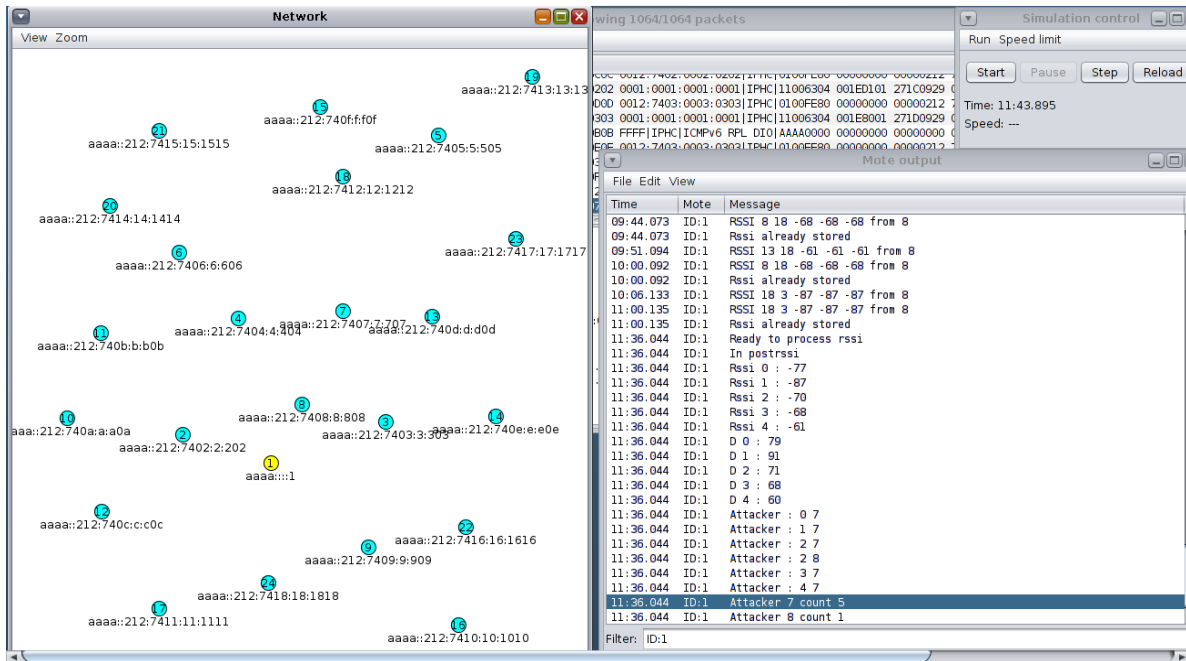


Fig. 4: Actual simulation showing detection of Wormhole attack

B. Energy Consumption

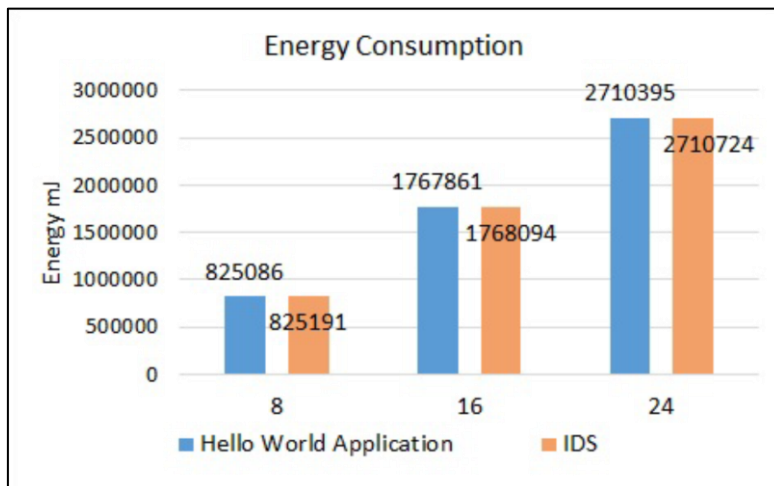


Fig. 5: Comparison of Energy Consumption

XI. CONCLUSION

IoT is very emerging technology but with that also many security threads. So, it is necessary to detect and prevent threats. We will define the propose model and that will use basically for the Intrusion Detection and Prevention techniques to stop attacks or malicious activity in Internet of Things network. In this system use signature based solution to provide security for Internet of Things Network. This system is beneficial for identifying new security threats and according to finding new prevention steps against those threats.

ACKNOWLEDGEMENTS

We are thankful to Mr. Aditya Kumar Sinha and Mr. Gardas Naresh Kumar for the useful discussions and valuable suggestions.

REFERENCES

- [1] Bashir, U. & M. Chachoo (2014). Intrusion detection and prevention system: Challenges & opportunities. In Computing for Sustainable Global Development (INDIACom), 2014 International Conference on, pp. 806–809. IEEE.

- [2] Dali, L., A. Bentajer, E. Abdelmajid, K. Abouelmehdi, H. Elsayed, E. Fatiha, & B. Abderahim (2015). A survey of intrusion detection system. In *Web Applications and Networking (WSWAN), 2015 2nd World Symposium on*, pp. 1–6. IEEE.
- [3] Hossain, M. M., M. Fotouhi, & R. Hasan (2015). Towards an analysis of security issues, challenges, and open problems in the internet of things. In *2015 IEEE World Congress on Services*, pp. 21–28. IEEE.
- [4] Jing, Q., A. V. Vasilakos, J. Wan, J. Lu, & D. Qiu (2014). Security of the internet of things: Perspectives and challenges. *Wireless Networks* 20(8), 2481–2501.
- [5] Kumar, S. A., T. Vealey, & H. Srivastava (2016). Security in internet of things: Challenges, solutions and future directions. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*, pp. 5772–5781. IEEE.
- [6] Rolf, O. *Security technologies for the World Wide Web*. Boston, MA: Artech House, 381.
- [7] Sonar, K. & H. Upadhyay (2016). An approach to secure internet of things against ddos. In *Proceedings of International Conference on ICT for Sustainable Development*, pp. 367–376. Springer.