IoT Applications and Contiki OS

[1]Brijesh Jajal, https://orcid.org/0000-0002-5892-2222
[1]Prakash Meena, http://orcid.org/0009-0009-3951-4555
[1]*Department of Computer Sciences and Engineering, Institute of Advanced Research, Gandhinagar*

Corresponding Author: Brijesh Jajal (brijesh.jajal@iar.ac.in), prakashmeena.phd2022@iar.ac.in

[1]

***Abstract*— The opportunity presented by the Internet of Things (IoT) spans across multiple industries and businesses. IoT represents a network of interconnected devices that collect crucial physical data and analyze it in the cloud to provide valuable business insights. Numerous companies are focusing on IoT and integrating connectivity into their future products and services. To ensure the success of the Internet of Things (IoT) market, it is essential to address three key challenges: technological, business, and societal. These challenges are relevant not only to IoT but also to any emerging technological trend.**

Contiki Os with Cooja Simulator provides the environment to build and test the IoT device before deployment. Here, we explore the Contiki Cooja simulator and analyze the Packet capture during Simulations. The Experiment result will be helpful for other researchers to work in this area.

Index Terms*— Contiki OS, Cooja Simulator, *IoT

I. INTRODUCTION

In the coming five years, there will be significant potential in the Internet of Things. Despite the precise functioning of smart objects, there remains a need for further development in IoT security. Currently, many IoT devices are rushed to market without considering essential privacy and security measures, leading to inherent insecurity.

The Internet of Things (IoT) comprises Internet-connected devices capable of sensing, communicating, and responding to environmental changes. There are billions of these devices linked to the Internet to share data with each other and/or their infrastructure. IoT holds the potential to facilitate a wide range of intelligent services across various aspects of our daily lives and enhance overall quality of life.

A. Internet of Things

Objects with unique identities communicate with each other through the internet, forming the Internet of Things. This has opened up a wide range of applications, such as home automation, which enhances human comfort and security. Security is a crucial aspect that needs careful consideration. The Internet has experienced rapid growth in recent years, significantly impacting human life by improving connectivity and communication. Internet technology can be leveraged to connect everyday objects, leading to the expansion of Internet services known as the Internet of Things. IoT Applications are shown in Figure 1.

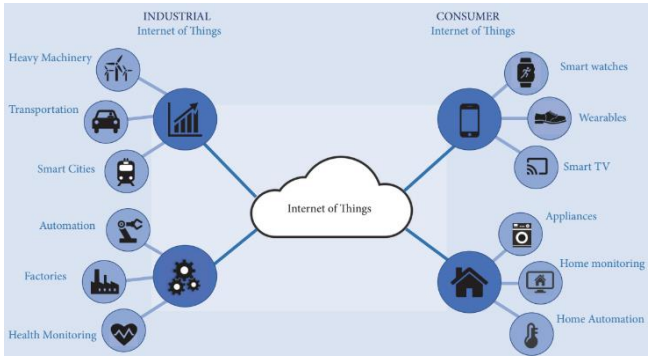


Fig. 1 Applications of the Internet of Things.[1]

B. Major Challenges Facing IoT

Ahmed Banafa's article "Three Major Challenges Facing IoT" was published on March 14, 2017, in the IEEE Internet of Things. In this article, the author outlines three key hurdles that the Internet of Things (IoT) needs to surmount in order to realize its complete potential. These challenges include:

Security: The expansion of IoT devices broadens the scope for cybercriminal attacks. Numerous IoT devices have inadequate security measures, leaving them open to hacking, data breaches, and other cyber risks. It is crucial to guarantee comprehensive security, which encompasses secure communication protocols, frequent software updates, and robust authentication mechanisms.

Interoperability: Ensuring smooth communication and collaboration among IoT devices from various manufacturers poses a major challenge due to the wide range of devices available. Common protocols and interfaces are necessary to establish standardization and enable interoperability. Without these, the complete potential of IoT in terms of data sharing and collective intelligence cannot be achieved.

Scalability: The infrastructure must expand in tandem with the rapidly increasing number of IoT devices, encompassing network bandwidth, data storage, and processing power. Effectively handling the massive amount of data produced by IoT devices and guaranteeing consistent, immediate processing and analysis is a multifaceted endeavor that demands sophisticated solutions. These obstacles underscore the requirement for continuous research, advancement, and

cooperation among invested parties to construct a secure, interoperable, and expandable IoT ecosystem.

Fig. 2: Challenges of the Internet of Things.[2]

C. Risks and challenges in IoT [3]

Navigating the Internet of Things (IoT) involves addressing various risks and challenges for both organizations and individuals. Below are some critical areas of concern:

Security Risks

Vulnerabilities: IoT devices frequently do not have strong security capabilities, leaving them vulnerable to hacking and unauthorized entry. A lot of devices come with default passwords or do not receive regular security updates.

Data Breaches: The collection and transmission of data by multiple devices heightens the risk of data breaches. Entry points into larger networks can be facilitated by compromised devices.

Botnets: IoT devices that have been infected can come together to create botnets, which can then be used to carry out distributed denial-of-service (DDoS) attacks. One well-known instance of this is the Mirai botnet.

Privacy Concerns

Data Collection: Concerns about user privacy are often raised due to the extensive amount of personal data collected by IoT devices. The data collected can encompass sensitive information like health metrics, location data, and usage patterns.

Surveillance: IoT devices are so widespread that they could result in more surveillance by either corporations or governments, which might violate the privacy rights of individuals.

Interoperability and Standards

Lack of Standards: The array of devices in the IoT ecosystem comes from different producers, frequently utilizing diverse communication protocols and standards, which can result in challenges with interoperability.

Integration Challenges: Integrating current systems with IoT devices can be both expensive and complicated, particularly if the devices do not comply with established standards.

Data Management

Volume of Data: Dealing with the massive amount of data generated by IoT presents difficulties in storing, organizing, and analyzing it. Efficiently managing this data requires organizations to have a strong infrastructure in place.

Data Quality: It is essential to guarantee the precision and dependability of data gathered from IoT devices to enable well-informed decision-making. Inaccurate data quality can result in erroneous conclusions and decision-making.

Regulatory and Legal Issues

Compliance: Navigating the regulations for data privacy and security can be complicated for companies that operate in multiple jurisdictions, as different regions have their own rules.

Liability: It can be difficult to establish who is responsible for IoT device malfunctions or security breaches, particularly when there are multiple parties (such as manufacturers, service providers, and users) involved.

Technical Challenges

Power Consumption: Batteries are essential for numerous IoT devices, so it's crucial to have energy-efficient designs in order to extend battery life. This is particularly important for devices located in remote or hard-to-reach areas.

Connectivity: Ensuring that IoT devices have dependable and uninterrupted connectivity is crucial for their proper functioning. Problems with connectivity can cause disruptions in the performance and dependability of these devices.

D. Simple IoT Network

The basic structure of an IoT consists of three layers: the physical resource layer, the network layer, and the data application layer, as shown in the illustration. The physical layer comprises sensors and actuators that use different communication devices to collect real-time data. The network layer encompasses various networking protocols and technologies, integrating them to establish a secure communication channel among network devices. This layer enables direct communication between devices to ensure network security and quality of service (QoS) [4].

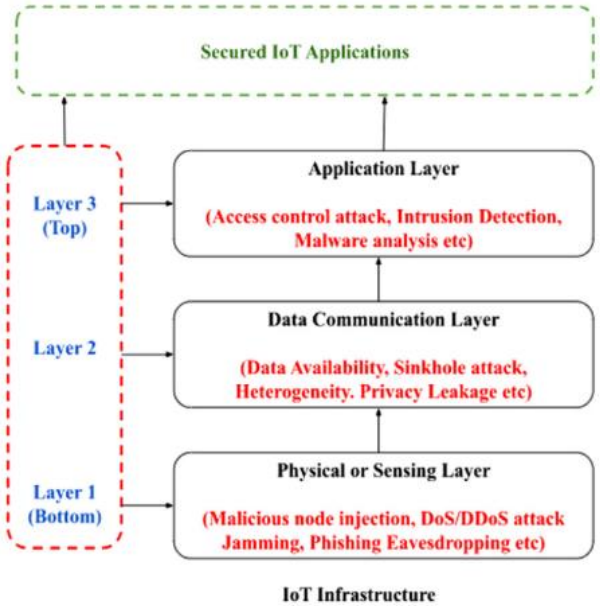


Fig. 3. The architecture of IoT consists of three layers [4].

The Application Layer provides services tailored to specific applications, such as smart cities and smart healthcare, using ML algorithms. It is a crucial part of the IoT network and is susceptible to security breaches. The ML algorithm utilized in this layer is responsible for ensuring the security and dependability of the IoT network.

II. MATERIALS AND METHODS

The Contiki OS is an operating system for IoT devices, specifically created to assist networked devices with limited resources. It is coded in C and focuses on efficient memory usage and power consumption. It is commonly configured to run on as little as 2 kilobytes of RAM and 60 kilobytes of ROM at 1 MHz [5].

Based on the 2017 IoT developer survey [6], approximately 13.4 million devices currently utilize Contiki, and this number is projected to increase steadily. Contiki is specifically designed to enable the connection of small, battery-powered devices to the internet, offering a lightweight implementation for various popular communication standards such as IEEE 802.15.4, 6LoWPAN, CoAP, MQTT, TSCH, and RPL. Furthermore, Contiki boasts a hardware-independent software infrastructure, with the core system providing minimalistic abstraction. This design supports system portability, allowing for additional platform support to be implemented in libraries and services on top of Contiki's adaptable architecture.

COOJA [7] functions as a Contiki network simulator and distinguishes itself from other emulators by enabling cross-level simulation in WSN. It facilitates simultaneous simulation from the low level, pertaining to sensor node hardware, to the high level, encompassing node behavior. This simulation environment allows developers to observe their applications running in large-scale networks and fine-tune the emulated hardware in great detail [8].

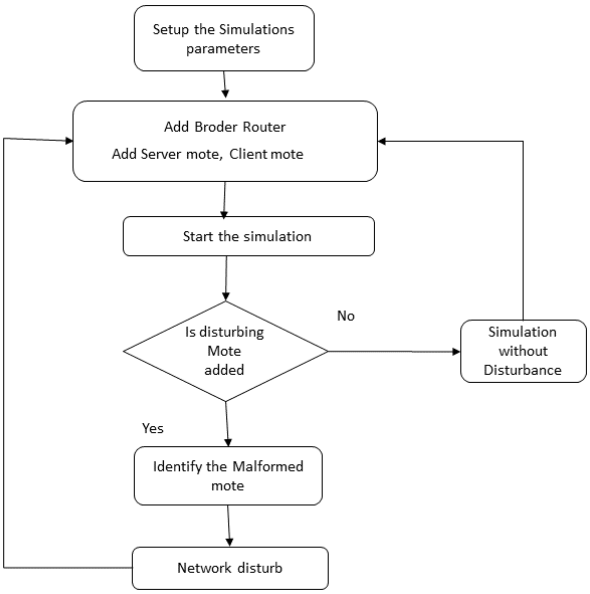


Fig. 4 The process of detecting intrusions in wireless sensor networks

III. RESULTS & DISCUSSION

Fig. 5 Actual Simulation and Other Author Simulations Screenshots

In accordance with Figure 4, we conducted an experiment to simulate the behavior of one Server, four Clients, and one Border Router. The results, presented in Figure 5, compare the output with a simulated network containing both malicious and non-malicious motes [9]. The nodes are efficiently connected to both the Server node and the disturber node. After generating the pcap file, we analyzed it using Wireshark. The findings, displayed in Figure 6, reveal the presence of abnormal node activity during communication between nodes.

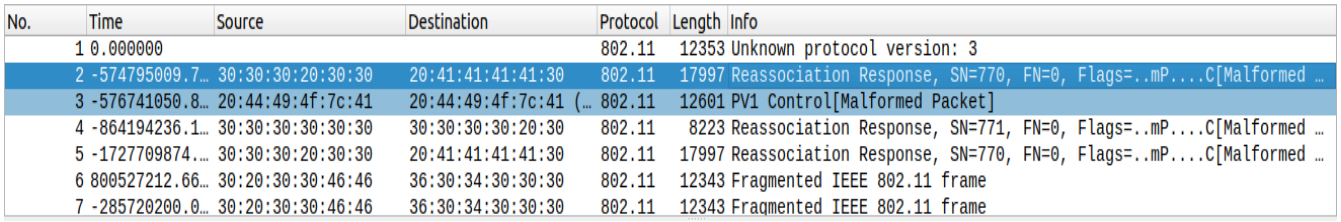
A border router connects a regular IP with the RPL 6LoWPAN [10,11] network. In the Contiki–Cooja simulation environment, a network's border router is located at the network's edge. The BR also works as a gateway to connect two different networks. In our simulation, we should write a command line to start connecting BR and the cloud.

The output shows the Node behavior with the time and protocol used for it. The network process is disturbed due to the disturbing node activity.

IV. CONCLUSION

The challenges of securing IoT devices were assessed in this paper through various approaches. Our comprehension of the IoT and its application challenges is thorough. We experimented with Contiki OS and the Cooja simulator. We use Border router nodes, server nodes, and client nodes. We understand the simulation process and perform several experiments to get a malformed node. Figure 6 shows the network traffic “pcap” with malicious activity as the result of the simulation.

In the future, various attack experiments can be conducted using Contiki and Cooja simulators. The improvement in the early attack identification using simulations is identified as a future scope.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			802.11	12353	Unknown protocol version: 3
2	-574795009.7…	30:30:30:20:30:30	20:41:41:41:41:30	802.11	17997	Reassociation Response, SN=770, FN=0, Flags=..mP....C[Malformed …
3	-576741050.8…	20:44:49:4f:7c:41	20:44:49:4f:7c:41 (…	802.11	12601	PV1 Control[Malformed Packet]
4	-864194236.1…	30:30:30:30:30:30	30:30:30:30:20:30	802.11	8223	Reassociation Response, SN=771, FN=0, Flags=..mP....C[Malformed …
5	-1727709874.…	30:30:30:20:30:30	20:41:41:41:41:30	802.11	17997	Reassociation Response, SN=770, FN=0, Flags=..mP....C[Malformed …
6	800527212.66…	30:20:30:30:46:46	36:30:34:30:30:30	802.11	12343	Fragmented IEEE 802.11 frame
7	-285720200.0…	30:20:30:30:46:46	36:30:34:30:30:30	802.11	12343	Fragmented IEEE 802.11 frame

Fig. 6. Pcap file Analysis using Wireshark

REFERENCES

[1] Mohamed Seliem, Khalid Elgazzar, and Kasem Khalil "Towards Privacy-Preserving IoT Environments: A Survey" Hindawi Wireless Communications and Mobile Computing Volume 2018, Article ID 1032761, 15 pages https://doi.org/10.1155/2018/1032761

[2] Ahmed Banafa Three Major Challenges Facing IoT - IEEE Internet of Things March 14, 2017 https://iot.ieee.org/articles publications/newsletter/march-2017/three-major- challenges-facing-iot.html

[3] What is the Internet of Things (IoT)? https://www.ibm.com/topics/internet-of-things

[4] Vinay Gugueoth, Sunitha Safavat, Sachin Shetty "Security of Internet of Things (IoT) Using Federated Learning and Deep Learning — Recent Advancements, Issues and Prospects" https://doi.org/10.1016/j.icte.2023.03.006 2405-9595/© 2023.

[5] A. Dunkels, B. Gronvall, and T. Voigt. Contiki-a lightweight and flexible operating system for tiny networked sensors. In Local Computer Networks, 2004. 29th Annual IEEE International Conference on, pages 455–462. IEEE, 2004.

[6] I. Skerrett. IoT Developer Survey 2017. https://www.slideshare.net/IanSkerrett/iot-developer-survey-2017.

[7] Mochammad Ichsan Rahmat Sanjaya,Aji Gautama Putrada, Vera Suryani "Anomaly Detection in IoT with Cooja Simulator" e-Proceeding of Engineering : Vol.8, No.2 April 2021 | Page 2977 ISSN : 2355-9365

[8] Jack McBride Budi Arief Julio Hernandez-Castro "Security Analysis of Contiki IoT Operating System "International Conference on Embedded Wireless Systems and Networks (EWSN) 2018 14–16 February, Madrid, Spain ISBN: 978-0-9949886-2-1

[9] F. Osterlind, A. Dunkels, J. Eriksson, N. Finne and T. Voigt, "Cross-Level Sensor Network Simulation with COOJA," Proceedings. 2006 31st IEEE Conference on Local Computer Networks, Tampa, FL, USA, 2006, pp. 641-648, doi: 10.1109/LCN.2006.322172.

[10] Manjula C Belavagi, Balachandra Muniyal, "Multiple intrusion detection in RPL based networks "International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 1, February 2020, pp. 467~476 ISSN: 2088-8708, DOI: 10.11591/ijece. v10i1.pp467-476

[11] W. Mardini, et al., "Comprehensive Performance Analysis of RPL Objective Functions in IoT Networks," International Journal of Communication Networks and Information Security (IJCNIS), vol. 9, pp. 323-332, 2017.

[12] W. Tang, et al., "Analysis and optimization strategy of multipath RPL-Based on the COOJA simulator," Int. J. Comput. Sci., vol. 11, pp. 27-30, 2014.