LoPT : LoRa Penetration Testing Tool

Smile Manuel J, Anatha Narayanan V, Sethumadhavan M

Abstract— ***The advent of Wireless technologies and IOT are currently ruling the modern world. Everything is going to become Things in future. As the technology progresses , the security of those technologies must also progress with an steady rate. Security tools which will help us to analyze these advanced security enhancements and protocols implemented. In this study , we are going to implement new security tool which concentrates on penetration testing of one such IOT protocol. This tool concentrates on the protocol named LoRa used for wireless long range communication in IOT. The proposed tool will explore all the possible attacks on LoRa protocol which we will see about in detail in the upcoming sections. LoPT is a new penetration testing tool which will work on LoRa (Long Range),a wireless standard used for long range low power communication on IOT devices primarily. This newly bloomed flower performs an effective domination on the field of IOT. Currently there is no existing penetration testing tool for LoRa. Though LoRa has its inbuilt security , there are major vulnerabilities which can be explored . This tool is built primarily on the concept of There's no such thing as 100***

Index Terms— ***LoRa , Pentest Tool for LoRa , LoRa Attack tool, LoRa vulnerabilities explorer***

1. INTRODUCTION

Most of the security loopholes/attacks happen due to improper configuration in the system ,their protocol and not identifying the pre-existing vulnerabilities . Addressing this case , where we have pentest tools. The penetration tools serves this purpose in the better way. What is penetration testing and why it does helps us in a better way. Penetration Testing is the methodology to find security vulnerabilities that an attacker could exploit. In our study, we are using the vulnerabilities of LoRa to create a new tool. The tool can be automated with software applications or performed manually. Pentesting is the process involves information gathering ,identifying possible entry points , attempting to break in – either virtually or for real – and reporting back the findings. The objective is to identify and objectify security weaknesses in the implementation ,protocol ,testing security policy, its adherence to compliance requirements and its organization ability to threat response. As IOT sector has been grown widely in every homes and industries , the new blooming flower LoRa needs an security tool. So finding its weakness after implementation in different sector is our primary goal which is address in this paper in form of LoPT tool.

2. BACKGROUND STUDY

2.1. LoRa

LoRa is a Wireless Communication .This technology is long-range communication especially designed for IOT networks. It is one of LPWAN protocol competed against others. It can transmit possible 10km+ by trading off data rate. It uses free band for communication. This is suitable for only applications that can tolerate delays. It uses free bands like like 169 MHz, 433 MHz, 868 MHz (Europe) and 915 MHz (North America).Though it is an LoRa uses chirp spread spectrum for commercial usage with low-cost implementation. LoRas spread spectrum technology is derived from chirp spread spectrum (CSS). LoRa chipsets have reduced power consumption, increased transmission power. The chipset also consume low power compared to other chipsets used for communications. LoRa devices uses timestamps and geo-coordinates to triangulates its positions of devices and gateways. LoRa permits long-range connectivity for IOT devices. They have largely utilized over different industries in huge scale .

2.2. LoRaPHY

It is an proprietary protocol , there is no freely available documentation about this technology .LoRa trades of its data rate for sensitivity with fixed channel bandwidth . It selects the amount of spread used which in turn selects the fixed channel bandwidth. Spreading factor determines the data rate and dictates the sensitivity of a radio. LoRas Forward error correction coding will improve resilience against interference. LoRa's high range is characterized by extremely high wireless link budgets, around 155 dB to 170 dB

2.2.1. LoRaWAN.

LoRa defines the lower physical layer and LoRaWAN defines the upper networking layers. Lo- RaWAN is a media access control (MAC) layer protocol but acts mainly as a network layer protocol. It usually manages communication between LPWAN gateways and end-node devices. It also acts as routing protocol for end-node devices. LoRaWAN is responsible for communication frequencies, data rate and power for all devices. Asynchronous data transmission and send only when data is available. Data is received by multiple gateways which forward the data packets to a centralized network server. The network server performs security checks and also duplicate packets. Data is forwarded to application servers. We find some issues related to sending acknowledgements

Revised Manuscript Received on July 18, 2019.

Smile Manuel J, TIFAC-CORE IN Cyber Security Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. (E-mail: smj1995@protonmail.com)

Anatha Narayanan V, TIFAC-CORE IN Cyber Security Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. (E-mail: veluananthu@gmail.com)

Sethumadhavan M, TIFAC-CORE IN Cyber Security Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. (E-mail: m_sethu@cb.amrita.edu)

Retrieval Number: I10810789S219/19©BEIESP
DOI : 10.35940/ijitee.I1081.0789S219

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

2.3. Related Works

Only small amount of works related to LoRa are done with respective to security. Every works constitutes what changes can be done to the existing classes of LoRa networks to upgrade its security. We dont have existing architecture to explore LoRa with clarity.

In one paper [1] named Evaluating LoRa and Wifi Jamming ,there are giving subject matter expertise on how to jam any radio signals . The library which they are using GNU radio which is publicly available public library can be used effectively for our purpose. They are also using HACKRF , a hardware based radio hacking tool utilized all over featured in Def Con , Black hat Conferences establishing its authority in the field of radio hacking. In the paper [2] Security of LoRaWAN v 1.1 in Backward compatibility Scenarios, there studied about the various attacks possible due to backward compatibility of LoRaWAN. How theyll use this backward compatibility to attack the environment is explained clearly. In book [3] Attacking and Defending LoRa systems ,it clearly explains lot about LoRa and its defense mechanism available.

The paper [4],explains the vulnerability analysis of LoRaWAN.From this reading we understood the major loopholes which can be exploited by the tool we are addressing to create.

For detection of Malicious attack on wireless ad-hoc network are given through this [5]paper.As LoRa also comes under wireless , malicious attackss detections mechanisms are been learnt from this paper.

We majorly concentrates on finding the vulnerabilities in LoRa protocol which is explained in this paper [6].Understanding this gives us an full overview about the major LoRa vulnerabilities. This paper [7] in depth analysis about the security analysis of LoRaWAN protocol.The protocol version 1.1 is improved version of old LoRaWAN protocol improving the older vulnerabilities.It gives major improvemnets to this protocol.

From the works of [8], we identify the potential methodologies to identify the jamming methods in LoRa.All these jamming methods are purely based upon certain scenarios.Jamming may not be possible in all the scenarios of LoRa.

To create an NIDS module for LoRa,we explored the IDS of wifi from the works of Athira [9]which proposed an clustering approach on this.The effective approach in LoRa is initially identified based on these works values.The NIDS formulated from the work paper by Danish published in 2018 IEEE conference [10].The paper clearly defines about jamming about detection using NIDS in LoRaWAN protocol.

2.4. Vulnerabilities and their Exploitations

In this section , [6]LoRa vulnerabilities and its exploitation methods are going to be explored. Different type of vulnerabilities existing in LoRa protocol. First identify all the basic asset of LoRa. The assets of LoRa are: Nwkskey,AppSkey,Appkey,DevNonce,AppNonce,Frmpayload ,Fcnt,ACK,MacCommands. We are identify in which these assets can be compromised. LoRa suffers major issues with their weaknesses in counters, decryption and MIC checking. Since its uses wireless transmission , over the air attacks are possible .Different scenarios are present through which it can be exploited successfully. The possible attacks of LoRa : Jamming Attacks, Replay Attacks , XORing cipher Text ,Eavesdropping ,Bit Flipping Attacks, ACK Spoofing ,DOS. These are few attacks possible on LoRa. The tool will implement most of these attacks and give mitigations steps based on that.

3. SETUP

3.1. Experimental Setup

We have setting up an test network with two LoRa nodes communicating with each other and one node as an attack vector. In our proposed architecture , we are using three LoRa devices integrated with Arduino board . The Arduino board uses communication program with another LoRa device setup. The third setup will act as an MITM module which will perform the attacks on the communication.Since using the LoRa module as an MITM device it will easy to interpret the radio signals successfully and easy to attack the network of LoRa devices

3.2. Lab Setup

We setup an initial level lab environment in IOT lab connecting two LoRa nodes with an raspberry pi and arduino node with is capable of capturing LoRa Packets and decoding the packets. Using this lab environment we tested the tool and got few results and working on the other results too.The lab setup is shown below in the figure 2

4. LOPT : TOOL ITS MODULES

LoPT tool is an specially designed tool only for attacking LoRa .We have different modules performing various tasks. Lets see about each and every module in detail below:

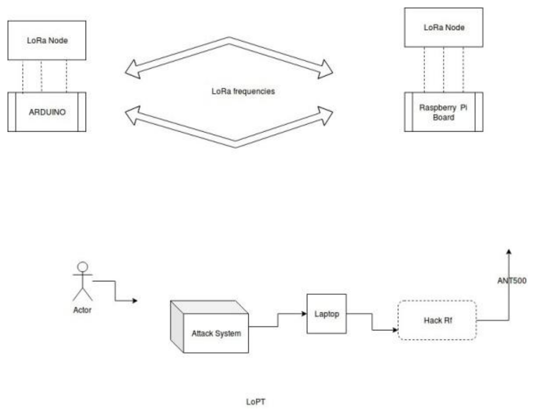


Figure 1. Experimental Setup of LoPT

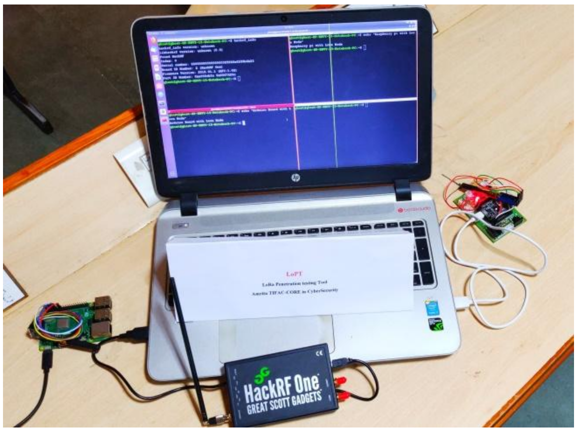


Figure 2. Lab Setup of LoPT

4.1. *Jammer Module*

It is a device which deliberately transmits signals on the same radio frequencies disrupting the communication between the LoRa devices and Gateway. When we consider about LoRa , the communication happens in three different frequencies , thus we need to module to jam three different frequencies. In the proposed tool , we are going to establish three different jammers like continuous jammer, selective jammer and timing based jammer. This tool will implement three different jammers . Continuous jammer will jam all the frequencies. Selective jammer will jam only the signals in the selected frequencies and timing based jammer will jam based on specific time. There will be set of time interval which will jammer will start its work and ends with specific time.

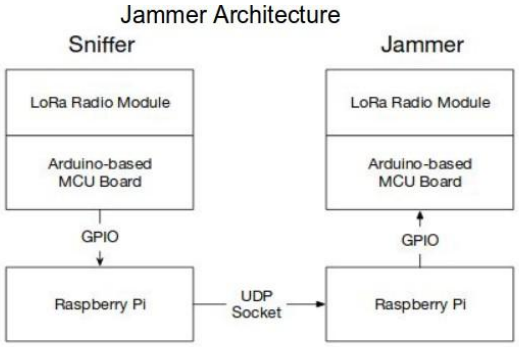


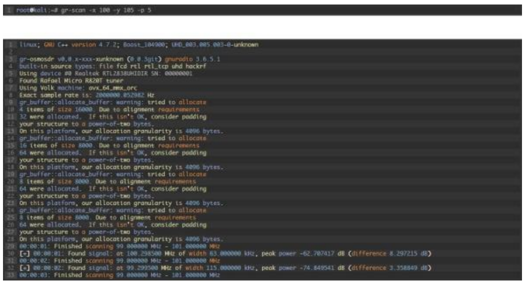
Figure 3. Jammer

4.2. *Sniffer Module*

Sniffer module is define in such a way to sniff all radio traffic in our specified LoRa frequencies. It sniffs all the traffic and it will be decoded with GNUradio library to understand its stream in a clear way. The traffic will be extracted with only LoRa packets which can be used to get necessary information on this.

4.3. *Scanner*

This module will scan for LoRa header and find the LoRa nodes in the premises. This scanner depends on the antenna power through which scanning is been done. Based on the antenna power , our scanner will work effectively.



```
root@kali:~# gr-scan -x 100 -y 105 -p 5
```

```
linux; GNU C++ version 4.7.2; Boost_104900; UHD_003.005.003-0-unknown

gr-osmosdr v0.0.x-xxx-xunknown (0.0.3git) gnuradio 3.6.5.1
built-in source types: file fcd rtl rtl_tcp uhd hackrf
Using device #0 Realtek RTL2838UHIDIR SN: 00000001
Found Rafael Micro R820T tuner
Using Volk machine: avx_64_mmx_orc
Exact sample rate is: 2000000.052982 Hz
gr_buffer::allocate_buffer: warning: tried to allocate
4 items of size 16000. Due to alignment requirements
32 were allocated.  If this isn't OK, consider padding
your structure to a power-of-two bytes.
On this platform, our allocation granularity is 4096 bytes.
gr_buffer::allocate_buffer: warning: tried to allocate
16 items of size 8000. Due to alignment requirements
64 were allocated.  If this isn't OK, consider padding
your structure to a power-of-two bytes.
On this platform, our allocation granularity is 4096 bytes.
gr_buffer::allocate_buffer: warning: tried to allocate
8 items of size 8000. Due to alignment requirements
64 were allocated.  If this isn't OK, consider padding
your structure to a power-of-two bytes.
On this platform, our allocation granularity is 4096 bytes.
gr_buffer::allocate_buffer: warning: tried to allocate
8 items of size 8000. Due to alignment requirements
64 were allocated.  If this isn't OK, consider padding
your structure to a power-of-two bytes.
On this platform, our allocation granularity is 4096 bytes.
00:00:01: Finished scanning 99.000000 MHz - 101.000000 MHz
[+] 00:00:01: Found signal: at 100.298500 MHz of width 63.000000 kHz, peak power -62.707417 dB (difference 8.297215 dB)
00:00:02: Finished scanning 99.000000 MHz - 101.000000 MHz
[+] 00:00:02: Found signal: at 99.299500 MHz of width 115.000000 kHz, peak power -74.849541 dB (difference 3.358849 dB)
00:00:03: Finished scanning 99.000000 MHz - 101.000000 MHz
```

Figure 4. LoRa Scan

4.4. *NIDS Module*

The major reason for this module , is to identify the attacks on LoRa network. So for organization using LoRa network , this module will be used to identify any attacks on their network.

4.5. *Attack Module*

This module is normally used to perform different attacks on the LoRa network . This module has different submodules which constitutes on various attacks possible on LoRa on certain conditions . Lets see about different attacks and their based conditions for this attack to succeed

4.5.1. *Replay Attacks.*

This attack will find vulnerability in counter fields. When frame counters are not properly handled in LoRa , it is subjected to replay attacks . Replay Attacks are nothing but sending old data packets which are captured during previous transmission again and again to attain specific expected outcome. To make this attack work , scenario present is frame counter checking must be disabled i.e, counter must not checked properly , leads to this attack possible.

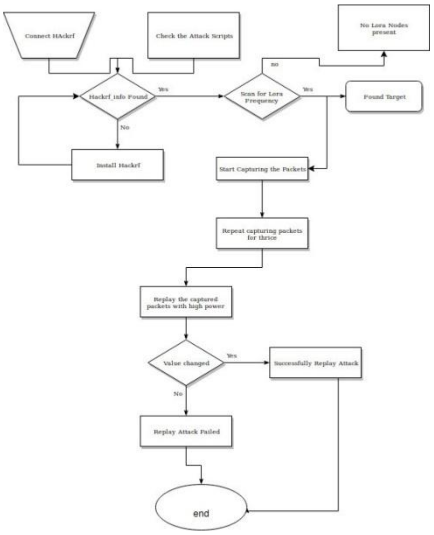


Figure 5. Replay Attack Flow

4.5.2. *DOS Attacks.*

DoS attacks aim to make an resource unavailable to its intended users by continuously flooding the network with repeated packets. In case of LoRa , DOS attacks is performed by repeatedly sending the crafted pay- load to the destination server or gateway making it not usable for other nodes.

4.5.3. Bit Flipping Attacks.

Bit flipping attacks flip bits between the network and application server .This attacks aims to successful manipulate messages which can not decrypt properly. Integrity is compromised because of this attack.So flipping the bit ,might actually alter the content of the message results in differ plaintext at receiver ends. If any operations are carried out at receiver end based on this input , it will be an disaster as someone manipulated the value

4.5.4. Eavesdropping.

Eavesdropping is one of the major attacks through which we are sniffing packets using MITM to get valuable information flowing in traffic .We have active and passive eavesdropping which varies slightly.In case of LoRa , this attack is designed to compromise the encryption method of LoRaWAN. By sniffing the wireless traffic between the gateway and the end device, the attacker can use the corresponding relationship between 2 messages with the same counter value to decrypt the ciphertext. After the attack, the attacker can compromise the confidentiality of the system, and obtain sensor data transmitted in the system. If LoRaWAN is used to transmit secret data, this attack can cause serious privacy issues. We already have sniffer module which can implement this attack successfully.

4.5.5. ACK Spoofing.

In LoRa, ACK is not checked pe- riodically. ACK are sent at delayed time period results in spoofing of ACK if an active attacker persists in the network. Since ACK delays persists in LoRa , it will easy for sending spoofed ACK results in various attacks.

4.5.6. Beacon Spoofing.

Beacon are normally to tell the presence of LoRa nodes . The liveness of LoRa nodes are sent as beacon nodes which are not encrypted . Since its not encrypted datas are sent as plaintext results in easy reading it. By Spoofing Beacon , we can act as other device to other node and initiate connection results in confidentiality loss of data.

4.5.7. UART Attacks.

UART attacks are normally done when they have physical access to the devices. We can easily read the information flow physically connecting UART pins on the LoRa end node to attify badge.Using UART we can stimulate side channel attacks ,power analysis attacks are feasible.

4.4.8. Fcnt Manipulation.

Fcnt is normally related to LoRa counter . By manipulating the counter value , we can make LoRa to wait for packet which will never transmitted in the network. Counter reinitialization also leads to several defects of packet handling makes to drop legitimate packet in the network.

4.6. Mitigation Module

This module gives information about mitigation of every successful attempts. This module clearly defines how to mitigate an successful attack.

We will give an report to the penetration testing team about the successful attempts made on the LoRa and we will mention the mitigation steps they have to take. If they patch those vulnerabilities, LoRa will become secure. Our goal to achieve in securing LoRa , has been one stepped closer. For every new vulnerabilities faced by LoRa , we have to create new modules in this tool and use it for further testing the LoRa system.

TABLE 1. MIGITATION MODULE

Sno	Attack Name	Where	Vulnerability	Mitigation Methodology
1	UART Attack	LoRa End Node	Using Serial connection , we can compro- mise LoRa data	Disabling UART debugging with high privileges
2	Bit Flipping Attacks	Application and Network Server	MIC not checked properly	Application Server must check MIC
3	Eavesdropping	Gateways	Counter issue Causes eavesdropping	Session keys must be changed periodically
4	ACK Spoofing	Gateways	ACK not send periodically	ACK must be send for every transmission
5	Beacon Spoofing	Node ,Gateways	Beacon are send to other nodes for live- ness of devices .Since its send over wireless it will be easy to spoof.	NIDS to identify some Beacon spoofing
6	Replay Attacks	Node ,Gateways	Counter Reuse , ABP Activation	End device resetting must be minimized.

TABLE 2. RESULT

S.No	Attack Name	Status	Details
1	Capture the packets	Successful	Able to capture the packets
2	Decode	Successful	LoPT successfully decodes the captured packet
3	Jammer	Failure	CSS protects from jamming the LoRa packets
4	UART Attack	Successful	Physical Attack using Attify badge
5	Replay Attack	Successful	We are able to replay the captured packet
6	Eavesdropping	Successful	Through physical connections we can eavesdrop the traffic

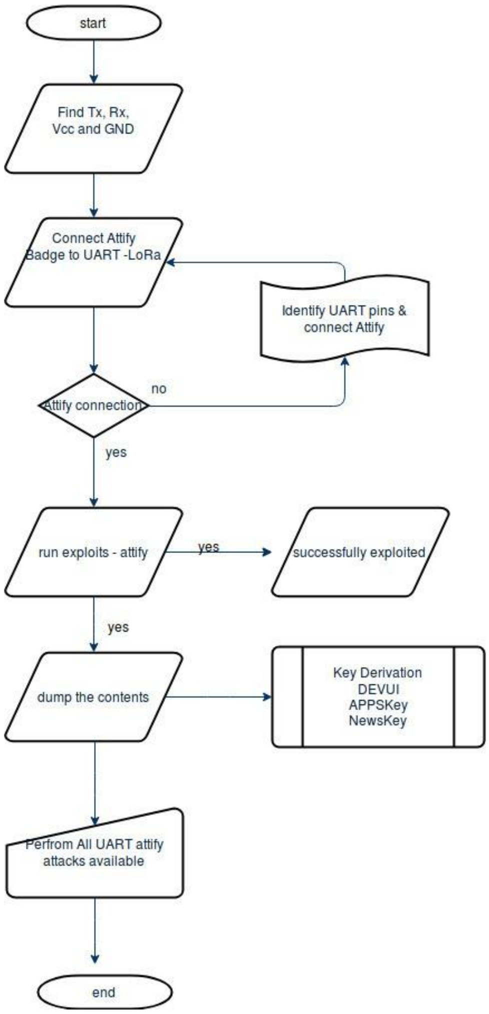


Figure 6. UART Attack Flow limitations.

This tool basically implements the attacks on LoRa Nodes not concentrated on the LoRaWAN structures. The attacks which can be done through this tool are UART attack,replay attacks ,eavesdropping , session key stealing

5. RESULTS

LoPT is an experimental tool which has been built for penetration testing on LoRa. Using this tool we are able to successfully capture the LoRa packets and decode the packets.The built jamming module is unable to jam the packets as due to advance chirp spreading spectrum technology utilized in LoRa. The present module concentrates on attacking the physical layer of the LoRa. Thus only few attacks are possible. The table below explains about the successfull and failures attacks on LoRa by LoPT:

6. CONCLUSION

We have successfully built LoRa pentest tool ,LoPT. This tool is proven to be effective in our experimental lab setup.The field trail for industrys or Smart cities are never been tried with this tool due to time limitations and resource through physical access.The tool can also be used for sniffing ,jamming the LoRa signals transmitted over different frequency channels.The tool also defines an NIDS module which has basic detection techniques to detect rogue devices. LoPT will be an effective pentest tool for LoRa based communication networks .Smart Cities where they used LoRa , we can use this tool to analyze the vulnerability status. Based on the user perspective , this tool can be used to exploit others network or checking strength of their known network. We have more areas to explore in this field of LoRa , which can be done in the future scope.

7. FUTURE SCOPE

In Future , we are planning to implement to new modules allowing future attacks can be integrated . The tool is written using python , thus it will be easy to extend into more modules tool. This tool will work well with the experimental setup , we need to check with industrial usecase. The tool has to be extended to use for industrial usage.We are also planning to implement Gateway Server attacks which will be future scope of attacks.As we know attacks on LoRa Node are very less as few security features and few areas to compromise the information are available in this.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

REFERENCES

1. A. Öst, “Evaluating lora and wifi jamming,” 2018.
2. T. C. Dönmez and E. Nigussie, “Security of lorawan v1. 1 in back- ward compatibility scenarios,” *Procedia computer science*, vol. 134, pp. 51–58, 2018.
3. R. Miller, “Lora the explorer–attacking and defending lora systems,” in *Information Security Conference–SyScan360*, 2016.
4. X. Yang, “Lorawan: Vulnerability analysis and practical exploitation,” *Delft University of Technology*, 2017.
5. J. Puthenkovilakam, “Malicious attack detection and prevention in ad hoc network based on real time operating system environment,”
6. E. Aras, G. S. Ramachandran, P. Lawrence, and D. Hughes, “Ex- ploring the security vulnerabilities of lora,” in *2017 3rd IEEE In- ternational Conference on Cybernetics (CYBCONF)*, pp. 1–6, IEEE, 2017.
7. I. Butun, N. Pereira, and M. Gidlund, “Analysis of lorawan v1. 1 security,” in *Proceedings of the 4th ACM MobiHoc Workshop on Experiences with the Design and Implementation of Smart Objects*, p. 5, ACM, 2018.
8. E. Aras, N. Small, G. S. Ramachandran, S. Delbruel, W. Joosen, and D. Hughes, “Selective jamming of lorawan using commodity hardware,” in *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pp. 363–372, ACM, 2017.
9. A. M. Nambiar, A. Vijayan, and A. Nandakumar, “Wireless intrusion detection based on different clustering approaches,” in *Proceedings of the 1st Amrita ACM-W Celebration on Women in Computing in India*, p. 42, ACM, 2010.
10. S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, and J. Rodriguez, “Network intrusion detection system for jamming attack in lorawan join procedure,” in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2018.