A study on Prototype Jammer System

KangWoon Hong
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
gwhong@etri.re.kr

Jong-Kook Lee
Defense ICT Convergence Research Sec.
ETRI
Daejeon, South Korea
raphael@etri.re.kr

Hea-Sook Park
Defense Safety Convergence Div.
ETRI
Daejeon, South Korea
parkhs@etri.re.kr

***Abstract*—This paper describes a jamming attack system that can be utilized to develop or evaluate jamming detection techniques. Recent jamming detection technologies utilize machine learning techniques to learn patterns of jamming types to generate jamming detection models, which are then applied to real-world environments to determine the presence of jamming attacks on real traffic data. Therefore, there is a need to develop a jamming attack system to generate training and test data for jamming detection models. To this end, we describe the structure, implementation, and verification of the jamming system, and then presents an expandable and switchable system structure that is easy to add and supplement functions.**

Keywords—Jammer, Architecture, Jamming Attack, Implementation

I. INTRODUCTION

The importance of wireless communication infrastructure is increasing due to the explosive proliferation of wireless services along with the activation of smart devices. Along with this, security threats to wireless communications are also recognized as a major problem due to the increasing reliance on wireless services. Because data transmission over wireless channels is inherently broadcast, the transmitted radio signals are vulnerable to external interference and malicious jamming attacks. In particular, jamming attacks on wireless networks are easy to execute compared to other types of attacks on other networks, so it is urgent to protect networks from such attacks, and due to the lack of protection mechanisms, jamming attacks can easily paralyze the network[4].

We need jamming detection technology to solve these problems or reduce the severity of the problem. Jamming detection technology plays an important role in maintaining the functionality, security, and resilience of wireless communication systems in various fields. Jamming attacks can cause disruption, data loss, degradation of service, or complete loss of connectivity to critical communications systems, and jamming detection technology can help you quickly identify attacks and restore communications integrity so that you can take countermeasures. Jamming can maliciously disrupt wireless communications in sensitive areas such as military installations, government facilities, or critical infrastructure. Jamming detection systems help security personnel identify and respond to jamming attempts and improve overall security. Jamming can interfere with emergency communication systems used for emergency services and public safety, hindering the work of first responders during disasters, accidents, or other critical situations, and detection techniques can ensure that communication channels remain operational during emergencies.

This paper describes a jamming attack system that can be utilized to develop or evaluate jamming detection techniques. Although this paper does not discuss jamming detection technologies, recent jamming detection technologies use machine learning techniques to learn patterns of jamming types to generate jamming detection models, which are then applied to real-world environments to determine whether a jamming attack has occurred on real traffic data. Therefore, the jamming attack system described in this paper is intended to be used to generate training and test data for jamming detection models.

This paper is organized as follows. Section 2 describes the jamming attack utilized to implement the jamming detection system and the implementation of a jammer using a commodity network adapter. Section 3 describes the structure of the jamming system, Section 4 describes the detailed implementation, Section 5 presents the jamming attack verification method, and Section 6 concludes.

II. RELATED WORKS

A. Jamming Attack

Jamming attacks degrade the performance of wireless communication systems such as WiFi networks and cellular networks, as well as cognitive radio, ZigBee, Bluetooth, vehicular, RFID, and GPS wireless networks, by introducing overhead that increases retransmissions and power consumption.

WiFi networks, the most common wireless network, generate more data traffic than cellular networks because they are easily accessible and ubiquitous. As such, WiFi networks can be a significant target for jamming attacks. Various types of jamming attacks are possible, ranging from general jamming attacks that can be utilized in other types of wireless networks to attacks against vulnerabilities in the MAC and PHY layer protocols of WiFi technology. Similar to WiFi networks, cellular networks are subject to general jamming attacks as well as vulnerabilities in MAC and PHY layer protocols that are specific to cellular networks. In addition, it is worth considering vulnerabilities in cognitive radio, ZigBee, Bluetooth, vehicular, RFID, and GPS wireless networks and the types of jamming attacks against them[1].

B. Raw Socket

A socket is an abstracted communication link that can be used to develop the interprocess communication programs regardless of the network's topology and networking scheme. Programs use them by making API calls to specify the address family, socket type, and protocol they use. Raw sockets extend the common sockets used for the interprocess communication at the transport layer and can also be used at the network layer and data link layer. This means that raw sockets can be used to forge and send packets by directly accessing information including headers below the network layer, which can be used for jamming attacks. In actual development, you can utilize lower-level libraries such as Socket, but you can also use frameworks such as Scapy to make the technology more accessible and easier to develop[5].

C. Flow-based programming

Flow-based programming is a component-oriented programming paradigm that defines applications as process nodes and message passing links, and represents them as process flows that exchange data through message passing. It provides a development concept that is easy to represent visually and allows developers to design programs easily.

NodeRED is a development environment platform that applies this concept and is popularly utilized in the IoT field. Usually, the data generated by physical sensors is processed through a series of processing on the NodeRED platform and then sent to the cloud to be utilized in another application. In this study, we use NodeRED for the initial implementation of the Jamming system. It has the advantage of being able to intuitively express the flow of a simple form of jamming attack to the network, or to deploy a jamming attack in response to the receipt of a certain type of packet, and to utilize NodeRED's already developed filter nodes[6].

III. PROTOTYPE JAMMER SYSTEM

A. Functional Architecture

The proposed jammer prototype system consists of three components, a jamming application, a network driver, and a wireless data link, as described in Figure 1. The jamming application organizes the jamming attack mechanism, the network driver generates the data that organizes the jamming attack, and the wireless data link physically transmits the data.

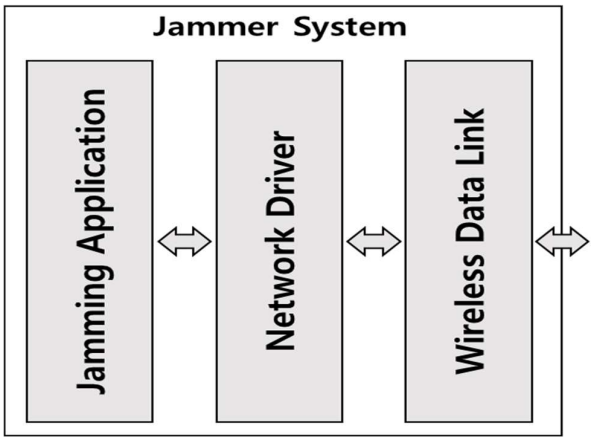

Fig. 1. Functional Architecture of Prototype Jammer System

Wireless data link performs the function of physically transmitting and receiving data in a wireless environment. Depending on the wireless standard, frequency, etc. used, it is implemented as a customized wireless system using general-purpose products such as wireless adapters or SDR (Software Defined Radio) products[2].

The network driver generates frames that constitute the jamming attack implemented by the jamming application. The network driver can optionally use raw sockets or SDR development tools as the wireless data link, depending on whether it uses a commodity network adapter or an SDR product.

The jamming application performs jamming attacks of the types supported by the jammer prototype system described in Section 3.1. Jamming applications can be implemented using the NodeRED platform using flow-based programming for system scalability and ease of development.

B. Jamming Attack

In the Jammer prototype system, a common jamming attack used in WiFi networks is targeted for implementation to verify the feasibility of the system. The detailed attacks and attack mechanisms of the general jamming type are as follows.

In constant jamming attack, the jammer broadcasts a powerful signal all the time. In reactive jamming attack, the jammer sends an interfering radio signal when it detects legitimate packets transmitted over the air. In deceptive jamming attack, the jammer lures legitimate devices to wait for meaningful radio signals, TaP(Truncate-after-Preamble). In random and periodic jamming attack, the jammer sends jamming signals for random periods and turns to sleep. In frequency sweeping jamming attack, the jammer sends jamming signals quickly switching to different channels.

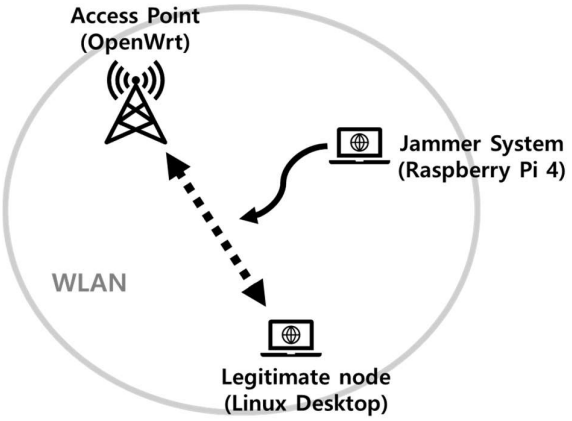

Fig. 2. Development and Test Environment

C. Implementation of Jamming Attack

To implement each of the jamming attack mechanisms described above, the values of parameters such as the strength of the jamming signal and the duration and frequency of jamming signal transmission must be determined. The parameter values are determined by referring to the values set and used by the Jamming module of NS-3[8].

Examples of parameter values for general jamming types are as follows.

TABLE I. PARAMETERS FOR GENERAL JAMMING ATTACK

Type of Jamming	*Parameters*	*Values*
Constant Jamming, Frequent Sweeping Jamming	Txpower	0.001 (=0 dBm)
	Duration	4 milliseconds
	Interval	0 millisecond
Random and Periodic Jamming	Txpower	0.001 (=0 dBm)
	Duration	600 milliseconds
	Interval	Randomly
Reactive Jamming	Txpower	0.001 (=0 dBm)
	Duration	5 milliseconds
	RX to TX switching delay	0.1 milliseconds
Deceptive Jamming	Packet length field	Announced: X bytes Actually: 2 bytes (<< X bytes)

The system proposed in this paper uses the above parameters to implement a jamming attack using Scapy. The development and test environment consists of a wireless access point and a normal user node that perform wireless communication based on the 802.11 standard between each other, and a jammer node that performs the jamming attack, as shown in Figure 2. The wireless access point installs the OpenWrt operating system to perform the wireless communication connection function, but it is also used in monitoring mode to check the data transmitted over the wireless by the jammer as well as the normal user node[9]. Software tools such as airmon, airodump, and tcpdump are used for monitoring. The Jammer node uses the Raspberry Pi hardware platform and perform jamming functions based on Scapy and Python[10].

D. Expandable and Switchable Jammer System

The jammer prototype system proposed in this paper consists of a jamming application for generic jamming attack, a raw socket based network driver, and a commodity WiFi adapter. In recent years, wireless communication systems using SDR devices have been actively developed, which can implement functions previously provided by analog hardware through software. In addition, when using a high-performance SDR device, timing issues can be satisfied during jamming, making it possible to implement intelligent jamming attacks such as MAC layer jamming attacks and covert jamming attacks in addition to generic jamming attacks. Therefore, as shown in Figure 3, a network driver and wireless adapter can be developed using the SDR device and GNU Radio SDR application development toolkit[7], and the jammer system can be further developed by linking with the NodeRED-based jamming application.

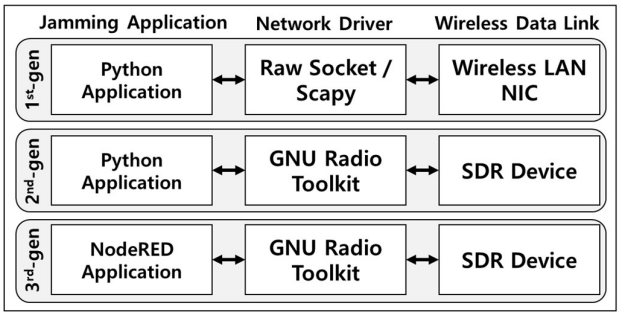

Fig. 3. Expandable and Switchable Jammer System

IV. Evaluation

As stated earlier, the purpose of the prototype jammer system proposed in this paper is to verify its feasibility. Therefore, we tried to propose an expandable system structure to accommodate additional and complementary features. In addition, to verify the implemented Jamming attack capabilities, we examined the RSS (Received Signal Strength) as shown in Figure 4 and confirmed that it shows a similar shape as in previous studies[3].

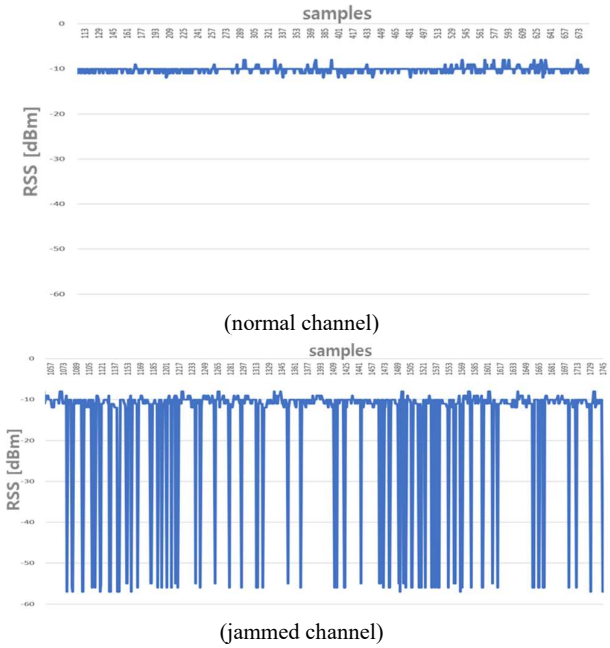

Fig. 4. Received Signal Strength in normal channel and jammed channel

V. Conclusion

In this paper, we presented a jamming attack system in terms of a scalable system structure that can be utilized to develop or verify jamming detection techniques. In addition, we present the implementation method and results of a prototype jamming system that includes common jamming attack types. By incorporating recent trends in wireless data links into the structure of the jammer system, we propose directions for future research.

Acknowledgment

This research was supported by the Challengeable Future Defense Technology Research and Development Program through the Agency For Defense Development(ADD) funded by the Defense Acquisition Program Administration(DAPA) in 2022(No.915064201)

References

[1] H. PIRAYESH and H. ZENG, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey.” IEEE communications surveys & tutorials, 2022, pp. 767-809.

[2] J. D. García, ‘‘Software defined radio for Wi-Fi jamming,’’ Villanova Univ., Villanova, PA, USA, Tech. Rep. 1, 2016, doi: 10.13140/RG.2.2.23772.90240.

[3] A. Hussain, N. Abughanam, J. Qadir, and A. Mohamed, ‘‘Jamming detection in IoT wireless networks: An edge-AI based approach,’’ in Proc. 12th Int. Conf. Internet Things, Nov. 2022, pp. 57–64.

[4] J. MYUNG, H. HEO, and J. PARK, “Joint beamforming and jamming for physical layer security,” ETRI Journal, 2015, pp. 898-905.

[5] https://scapy.net/

[6] https://nodered.org/

[7] https://www.gnuradio.org/

[8] https://www.nsnam.org/wiki/Wireless_jamming_model

[9] https://openwrt.org/

[10] https://www.raspberrypi.com/