eSWORD: Implementation of Wireless Jamming Attacks in a Real-World Emulated Network

Clifton Paul Robinson†, Leonardo Bonati†, Tara Van Nieuwstadt*, Teddy Reiss*, Pedram Johari†,
Michele Polese†, Hieu Nguyen*, Curtis Watson*, Tommaso Melodia†
†Institute for the Wireless Internet of Things, Northeastern University, Boston, MA, U.S.A.
E-mail: {robinson.c, l.bonati, p.johari, m.polese, melodia}@northeastern.edu
*The MITRE Corporation, Bedford, MA, U.S.A.
E-mail: {tvannieuwstadt, treiss, htnguyen, cmwatson}@mitre.org

***Abstract*—Jamming attacks have plagued wireless communication systems and will continue to do so going forward with technological advances. These attacks fall under the category of Electronic Warfare (EW), a continuously growing area in both attack and defense of the electromagnetic spectrum, with one subcategory being electronic attacks (EA). Jamming attacks fall under this specific subcategory of EW as they comprise adversarial signals that attempt to disrupt, deny, degrade, destroy, or deceive legitimate signals in the electromagnetic spectrum. While jamming is not going away, recent research advances have started to get the upper hand against these attacks by leveraging new methods and techniques, such as machine learning. However, testing such jamming solutions on a wide and realistic scale is a daunting task due to strict regulations on spectrum emissions. In this paper, we introduce *eSWORD* (emulation (of) Signal Warfare On Radio-frequency Devices), the first large-scale framework that allows users to safely conduct real-time and controlled jamming experiments with hardware-in-the-loop. This is done by integrating METEOR, an electronic warfare (EW) threat-emulating software developed by the MITRE Corporation, into the Colosseum wireless network emulator that enables large-scale experiments with up to 49 software-defined radio nodes. We compare the performance of *eSWORD* with that of real-world jamming systems by using an over-the-air wireless testbed (considering safe measures when conducting experiments). Our experimental results demonstrate that *eSWORD* achieves up to 98% accuracy in following throughput, signal-to-interference-plus-noise ratio, and link status patterns when compared to real-world jamming experiments, testifying to the high accuracy of the emulated *eSWORD* setup.**

I. Introduction

Electronic warfare (EW)—defined as the ability to use the electromagnetic spectrum to sense, protect, and communicate, as well as deny adversaries the means to disrupt and use these signals [1]—has continuously grown throughout the years as a major area in both attack and defense [1]. The importance of EW for both attack and defense applications is further confirmed by its steep market growth in recent years (worth $17 billion in 2020 alone, and expected to reach $21 billion by 2025 [2]). EW is divided into three major categories, each having many subcategories: (i) *Electronic Attack*, which utilizes electromagnetic energy as an offensive weapon in combat; (ii) *Electronic Protection*, used to protect personnel and equipment from the effects of the electromagnetic spectrum; and (iii) *Electronic Support*, where the focus is on the recognition and response to these threats to help detect enemy's electromagnetic weapons. In this paper, we primarily focus on the *Electronic Attack* area. Electronic attacks are any form of adversarial signal that attempts to disrupt, deny, degrade, destroy, or deceive signals on the electromagnetic spectrum [1]. One of the most common types of these attacks comes from the broad area of signal jamming, a type of denial of service (DoS) attack where malicious entities block legitimate communications by causing intentional signal interference [3].

Jamming attacks have plagued wireless communication systems for many years, and they continue to be a problem as technology evolves, as there is no single solution to handle this broad adversarial attack. However, in recent years, research solutions using novel techniques applied to jamming, e.g., machine learning, have started to spawn [4–7]. Although such solutions have started to get the upper hand on jamming [8], prototyping and testing them at scale and in realistic wireless environments is a daunting task because of the strict regulations on spectrum emissions. For example, the United States forbids any form of signal jamming since such signals pose a serious risk to public safety communications (e.g., they could prevent someone from making emergency calls) [9]. Even though some methods exist to validate jamming solutions, e.g., software simulations or experiments in anechoic chambers, they can hardly capture either the accuracy or the scale of real networks with actual hardware-in-the-loop (HITL). HITL offers the most benefits to jamming experiments as it enables *real*, non-synthetic signals over emulated channels with real hardware devices, and without causing harmful interference to public communications.

In this paper, we propose *eSWORD* (**e**mulation (of) **S**ignal **W**arfare **O**n **R**adio-frequency **D**evices), a first-of-its-kind, large-scale framework with HITL to conduct real-time, accurate tests of jamming signals on a wireless spectrum. *eSWORD* allows for the testing of different adversarial jamming scenarios on a wireless spectrum with *real* signals (both adversarial and legitimate) in a safe environment. We prototype *eSWORD* on the Colosseum wireless network emulator [10], a large-scale software-defined radio (SDR)-based testbed that allows users to evaluate solutions in realistic but controlled environments with HITL. We leverage this testbed to evaluate our solution at scale over a softwarized cellular network with 50 nodes

This work was partially supported by the U.S. National Science Foundation under grant CNS-1925601. Additional funding support was provided by the MITRE Corporation. Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-2965.

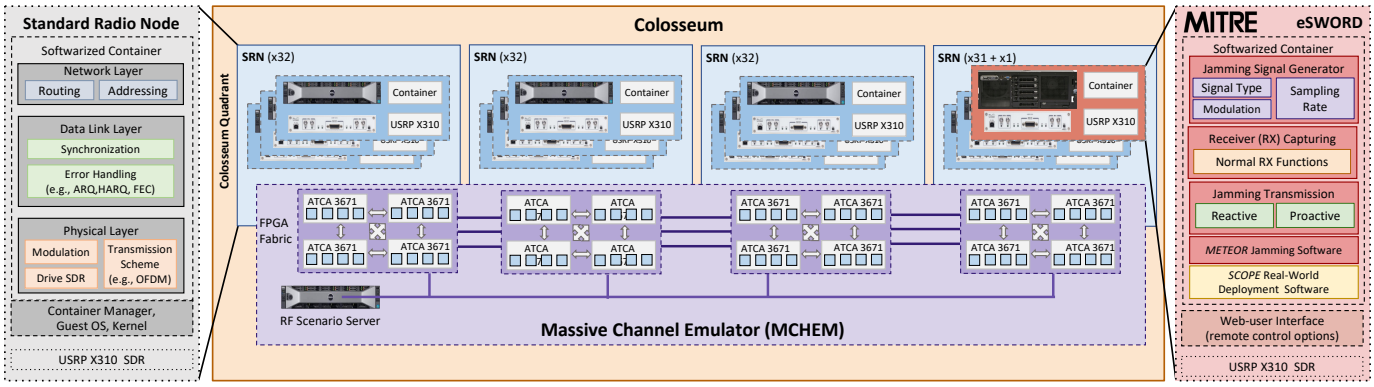

Fig. 1: Overview depicting how *eSWORD* is integrated into Colosseum, taking the place of one of the SRNs, allowing for the jamming software to be used.

shared among base stations, users, and jammer. Colosseum allows us to prototype *eSWORD* in a controlled environment without causing external interference to commercial devices. We compare the results obtained with *eSWORD* to those of real wireless jamming signals (collected ethically). We verify that *eSWORD* is able to provide accurate real-time results, e.g., *eSWORD*'s throughput follows a pattern with accuracy up to 98% when compared to real-world results. Finally, we perform a jamming experiment in a controlled over-the-air testbed in similarity to the *eSWORD*, and verify the accuracy of its results. To the best of our knowledge, *eSWORD* is the first jamming emulation system that makes it possible for researchers to evaluate solutions at an accurate network scale with HITL and in multiple emulated but realistic wireless environments provided by the Colosseum wireless network emulator.

The main contributions of this paper are as follows:

1) We create and prototype *eSWORD* (Fig. 1, explained in details in Section V), a framework that allows for the emulation of jamming in a wireless spectrum at scale (with up to 50 communicating nodes), where one of the nodes can be an adversarial jammer.
2) We show that *eSWORD* is able to generate multiple types of jamming signals using different signal types and modulations to allow for many unique types of attacks.
3) We compare *eSWORD* results with real-world jamming signals, demonstrating *eSWORD* emulation accuracy.

The remainder of the paper is organized as follows. Section II discusses the related work and research regarding this area. Section III lays out the jamming adversary we focused on in this paper. In Section IV, we discuss the *eSWORD* prototype and the components that create it. In Section V, we describe the testbed implementation, while experimental results are shown in Section VI. Finally, Section VII concludes the paper.

II. Related Work

Wireless jamming has been studied for many years by the research community. There is a constant ebb and flow with research surrounding it due to the fact this form of attack advances with the advancement of the technology. While attempting to implement new methods to protect against these attacks, a major focus is discovering how these signals impact the wireless networks as a whole [11, 12]. Overall, wireless jamming research can be put into three broad categories, (i) attack [11–17]; (ii) defense [3, 14, 18]; and (iii) detection [13, 19, 20].

Jamming attacks and defenses usually go hand-in-hand within the research community as defense techniques, such as signal detection and frequency hopping [3, 18], are investigated to mitigate the considered attacks [3, 14, 18]. In these experiments, there is a true focus on "knowing your enemy" by taking a deep dive into these sorts of attacks and seeing how they work within a network [11–13]. Large-scale WiFi research has been done in the past, showing how jamming attacks on commercial wireless solutions, such as those enabled by the IEEE 802.11 standard, deteriorate the network performance [11], and showing that high WiFi data rates are not resilient to jammers. Further research focuses on specific types of jamming implementations. The authors of [16] study selective jamming, where the adversary focuses on "high-value" targets by exploiting their knowledge of the network, while also proposing a prevention mechanism that neutralizes the inside knowledge of the attacker. Still a common jamming technique today, reactive jamming is instead known for its strategy and detection avoidance. For instance, the authors of [12] discuss the implications of this form of attack in wireless networks.

Jamming avoidance has become more advanced with the use of spread-spectrum techniques [3, 18, 21]. The two main techniques used today are frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS). The former allows for jamming avoidance as it can literally "jump" away from attacks by hopping to frequencies not affected by jammers [22]. The latter takes a different approach, using rapid phase transitions with the data, spreading it on a larger bandwidth, thus conferring it more resilience to jammers [23].

While extensive research surrounding jamming has been done throughout the years, to the best of our knowledge, existing implementations and techniques are tested either through software simulations or in small-scale setups. In this sense, our research takes a step forward by implementing and evaluating *eSWORD* on a large-scale testbed with hardware-in-the-loop. As opposed to software-based simulations, this gives us access to data inputs from real physical devices, i.e., SDRs, and allows for experiments in controlled, but realistic environments without compromising commercial systems.

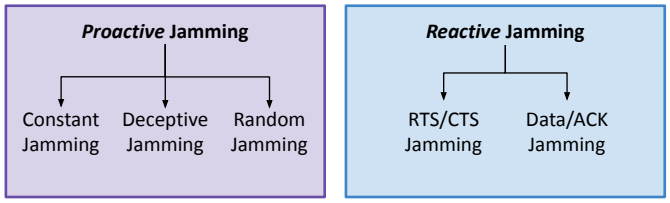

Fig. 2: Two broad categories of different jamming attacks.

III. The Adversary: Wireless Jamming

Jamming attacks have been exacerbated in recent years as the technology needed to create jamming signals has become more accessible and affordable [3]. Today, anyone with a SDR and a few lines of code can create a jammer that can deteriorate the performance of a wireless network, or even annihilate it. On a much larger scale, jamming has become a popular form of EW [24]. Such attacks can be coordinated better, with novel implementations that can take down large portions of cellular, GPS, and wireless networks in a deployed area.

Fig. 2 shows two of the most common categories of jamming attacks which is our focus in this paper. Proactive jamming is the most simple of the two, it happens when a signal is transmitting whether there is communication in a network or not [3]. Reactive jamming goes a step further, as jamming signals are only transmitted when communications are occurring in the network [12]. This makes it more difficult to detect adversaries as reactive jamming waits for the presence of data.

A proactive jammer works by placing the transmitters in a specific channel into non-operating mode, making that channel unusable [3]. A reactive jammer, instead, actively monitors a predetermined bandwidth and responds to specific packets or signals that are currently traveling in the air [12]. Unlike its proactive counterpart, a reactive jammer can be harder to detect as it targets on-air packets and can tune the time and spectrum location of the attack. Reactive jamming is also considered a stepping-stone, as it is the most common form of jamming that is used to implement more optimal jamming attacks [12].

An example of our reactive jammer on a 10MHz channel can be seen in Figure 3. In this example, a jamming signal with a bandwidth of 156KHz starts attacking the WiFi signal on the center frequency 2.378GHz, and after $\sim$100ms the WiFi signal shifts to the center frequency 2.382GHz, where the jammer shortly follows after it, sensing the change in energy location. This attack has direct impacts on the WiFi signal's transmissions, as when it avoids the signal has throughput values up to 11Mbps, but when the jammer catches it can drop all the way to 4Mbps. By using both proactive and reactive attacks, we cover a broad scope of knowledge within the attack area.

IV. Our Prototype: *eSWORD*

eSWORD is a software prototype that utilizes jamming software within a large-scale network emulator. The main goal of *eSWORD* is to provide a means to run large-scale jamming experiments in an accurate and safe environment.

Fig. 1 shows the high-level overview of our prototype ("*eSWORD* Device" in the figure). The prototype comes with a proprietary jamming signal generator, where the signal type, modulation, and sampling rate can be easily adjusted. Normal TX/RX functions are also included to transmit data, as well as jamming transmission capabilities for multiple forms of attacks. By utilizing this jamming software, we can create adversarial signals that work against practical real-world systems. As stated in Section III, our threat emulator focuses on proactive and reactive attacks. This allows for the implemented jammer on the emulator to give broad results that cover a multitude of similar attacks. As this threat emulator is designed to work in the real-world, commercial SDR hardware enables the use of *eSWORD* over-the-air on real wireless networks, granted the appropriate steps are taken to ensure safe transmissions.

Our prototype is controlled through a web interface that supports RESTful APIs and gives control of the SDR to the users. By using such an interface, users can control when data streams begin and end, as well as when jamming signals are transmitted. Within both the RX and TX, the center frequency, sampling rate, and gain can all be adjusted. In addition, a live spectrogram (see Fig. 3) can be started together with the RX stream to easily monitor the received signals in real-time.

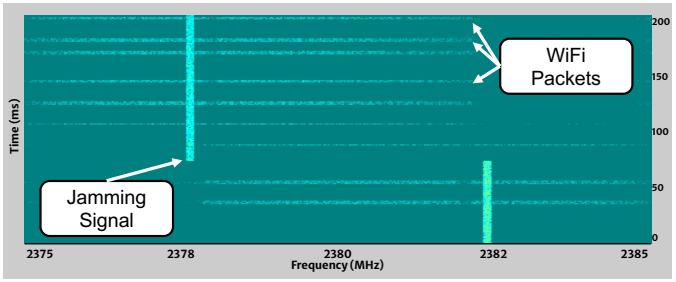

Fig. 3: An example of reactive jamming on frequency hopping WiFi signals.

A. Jamming Software & Attack Vector

Our prototype utilizes an EW threat-emulating software, called METEOR, developed by the MITRE Corporation [25]. METEOR is built with commercial off-the-shelf SDR, supporting software-defined capabilities and programmability. *eSWORD* uses the EW attack capabilities of METEOR, which include reactive and proactive jamming attacks in wireless scenarios. Such an EW attack could indeed be used in the wild to hamper or disrupt complex wireless communication systems.

METEOR offers a versatile jamming file generator that supports diverse types of modulated signals, shown in Table I. These different types of signals allow for multiple forms of jamming attacks to be created, including but not limited to constant jamming signals, pulsed signals, and narrowband or wideband signals. The specific signals we leverage for the

TABLE I: Types of jamming signals and modulations supported by METEOR.

Signal Type	Modulation
FSK	Frequency shift keying
ASK	Amplitude shift keying
MSK	Minimal shift keying
AWGN	White noise (barrage jamming)
Band Noise	Band-limited noise signal
Continuous-Phase	Continuous-phase frequency shift keying

attacks carried out in this paper are narrowband jamming signals with proactive and reactive capabilities. This variety of modulation types creates a large attack vector that allows for testing the resilience of different kinds of networks against specific attacks. On top of its signal generation capabilities, METEOR also allows users to upload their own custom files to use as jamming signals.

V. Experimental Testbed Setup

We implement *eSWORD* on the Colosseum wireless network emulator [10], a publicly available testbed that allows users to perform large-scale experiments with up to 128 programmable nodes and radio devices (see Fig. 1). Specifically, Colosseum is formed of two main blocks: (i) the Standard Radio Nodes (SRNs), and (ii) the massive channel emulator (MCHEM). The SRNs (shown in Fig. 1, top-middle) are 128 remotely accessible compute nodes that control a USRP X310 SDR each. These nodes can be leveraged to perform custom experiments through softwarized protocol stacks (Fig. 1, left) executed on them and used to control the SDRs that act as radio front-ends. MCHEM (Fig. 1, bottom-middle), instead, takes care of emulating channel conditions between every pair of SRNs by processing signals generated by the SDRs through FPGA-based Finite Impulse Response (FIR) filters. These FIR filters apply the channel impulse response of the Colosseum scenario selected by users to the SDR signals, thus emulating the actual real-world wireless scenario. We use METEOR (Fig. 1, right) to interfere with a network composed of 49 nodes implemented through the SCOPE framework [26]. This framework extends srsRAN—which allows users to deploy cellular protocol stacks on software-defined nodes and radios—with automated pipelines to swiftly run on the Colosseum testbed. Colosseum enables extensive testing environments and conditions through a set of diverse wireless scenarios representative of real-world urban cellular deployments, channels, and traffic demand.

To perform our jamming experiments, we integrated the METEOR node and dedicated SDR (a USRP X310) within Colosseum, which enables us to potentially jam any of the Colosseum nodes. In our experiments, we considered center frequencies of 980 MHz for the cellular uplink signals and 1020 MHz for the downlink signals. Fig. 1 gives an overview of our *eSWORD* prototype framework that integrates the METEOR jamming system into the Colosseum wireless network emulator. For the jammer to be used, the jamming software is flashed onto the FPGA of *eSWORD* SDR, and driven by a dedicated compute node. With METEOR being integrated to the channel emulator, it can operate similarly to the normal nodes on the Colosseum, except instead of being an SRN, it represents a jammer node that can jam the signals traveling across the scenario emulated by Colosseum. As of now, *eSWORD* includes a single jammer; however, multiple jammers can be integrated following a similar procedure if needed.

A. Node Placement within Testbed

To emulate a diverse set of wireless environments, we leveraged the large-scale urban cellular scenarios available on Colosseum [26]. These scenarios allow for real-world location testing, using base stations whose locations match the coordinates of commercial deployments, as well as a number of user equipment deployed in their surroundings. These locations correspond to Rome, Italy; Boston, U.S.; and Salt Lake City, U.S. A sample map of the locations of the base stations considered for the Boston area is shown in Fig. 4. This scenario includes 10 cellular base stations, and 40 cellular users (deployed in groups of 5, i.e., 1 base stations around 4 users in each cluster). Base stations and the users they are serving divide the network into clusters (see Fig. 4). By using these scenarios, we can test jamming impacts across different base stations, as well as move the jamming node to different locations within the scenario. In our experiments, a single node is replaced with a malicious node with jamming capabilities. This setup is able to show how a single jamming source impacts the initial user placement, as well as the base stations around it.

B. Over-The-Air Experimental Setup

We leverage the Arena testbed [27] to perform our over-the-air experiments. Arena consists of a grid of USRP X310 SDRs deployed in an indoor office environment. To conduct our real-time, non-emulated experiments, we use 3 of Arena SDRs and perform safe narrowband jamming experiments that do not interfere with any of the spectrum used by external applications. One of Arena SDRs acts as a receiver, one as a transmitter, and one as a jammer. The jamming signal used in this case is built to mimic the characteristics of the signals of the *eSWORD* Colosseum prototype. In this case, we collect channel throughput statistics and compare to those of the *eSWORD*.

VI. Experimental Results

The results collected in these experiments are designed to test the accuracy of *eSWORD*. The first part of these results compares the *eSWORD* prototype implemented on Colosseum with real-world jamming signals, while the second part discusses the impact on nodes in the emulated scenario. In both cases, *eSWORD* is used to jam a cellular network with 49 software-defined nodes (10 base stations and 39 users, see Section V).

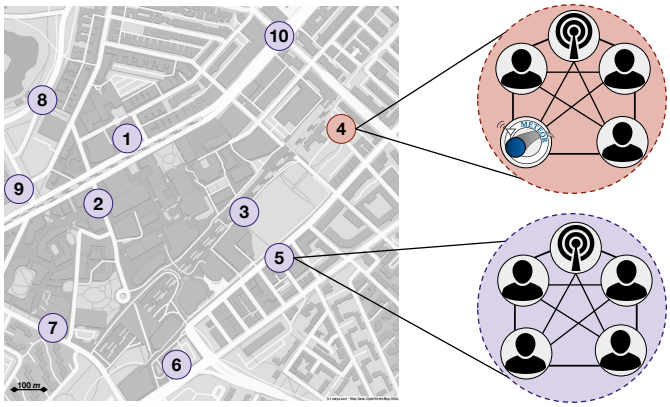

Fig. 4: The real-world example of node placement in Boston, with a jamming node located in cluster #4 taking a spot out of the 50 possible nodes.

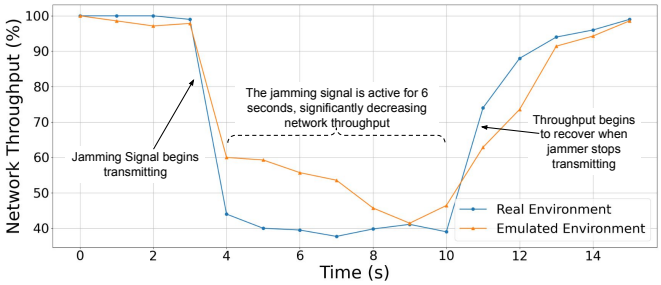

Fig. 5: A throughput example of a real-world network impacted by a jamming signal and the *eSWORD* emulated network impacted by the jamming signal. 100% refers to the throughput of the legitimate nodes in absence of the jammer.

A. Over-the-Air vs. Emulated Environment

In this section, we validate the accuracy of *eSWORD* prototype on the Colosseum emulator, comparing it with real-world—over-the-air—jamming signals, used as our baseline.

1) Jamming Signal Composition: The jamming signal for both real-world and emulation setups are constructed in the same manner (i.e., center frequency, sampling rate, etc.), allowing for accurate emulation, with the option of adjusting sampling rate, gain, and signal size. In this specific example, both signals are narrowband noise jammers using FSK modulation, focusing on disrupting a single channel's communication.

2) Channel Throughput Comparison: Throughput is one of the main metrics used to test the performance of a network. Fig. 5 shows the throughput (expressed as a percentage) in both the real and emulated networks over a 15-second window when a jammer is introduced. This jammer is stationary and holds the same power level while turned on. It can be seen that for both networks, the throughput stays near the maximum value (i.e., 100%) for the first 3 seconds of the experiments, until a narrowband jamming signal is introduced between seconds 3 and 4. Once the jammer is activated, the throughput significantly drops for both cases. The real network environment drops by almost 60% as the jammer interrupts the ongoing communications, while the drop in the emulated environment is slower, which can be attributed to the node locations differing in closeness, with the throughput decreasing by 40% within the first second. As the constant jamming signal continues, both networks drop to similar points (i.e., both having throughput drops near 60% of the original signal). Once the jammer is deactivated (second 10 of the experiment), both networks quickly recover back to their original throughput values. For the accuracy of the throughput between the two environments, the comparative accuracy of the emulated data is between 75% and 98% as shown in Fig. 5.

B. Impact on Radio Communication Performance

Emulated environments require more than just an accurate-looking jamming signal to claim they are correctly functioning. Indeed, there also needs to be actual cause and effect to the network and nodes as well (i.e., the way a jammer is set up impacts the network in different ways). As an example, the gain of the jamming signal has a direct impact on how a legitimate node is affected, as lower gains impact less than higher ones. This also determines whether a node will still be able to transmit while being affected by the jamming interference. Fig. 6 shows the real-time impact of different gains on a legitimate node. We consider how a jamming signal varying its gain from 0 to 32 dB (shown at the bottom of the figure) impacts the signal-to-interference-plus-noise ratio (SINR) of a legitimate node, and its link status, in a time window of 15 minutes (top portion of the figure). We notice that the SINR gradually decreases toward 0 with each increase in the jamming gain, showing the direct impact of the jammer on the legitimate node. Specifically, when the gain of the jammer is highest (between minutes 9 and 10), the link status of the legitimate node drops to 0, effectively causing the node to detach from the network (and not being able to communicate with the remaining nodes). As the jamming gain lowers, the SINR of the node improves, and the node is able to reconnect to the network. From this experiment, we notice that as the gain of the jammer increases by 5 dB at each time-step, the SINR of the legitimate node drops between 16% to 20% which shows an inverse correlation between the jamming power and the achievable SINR.

C. Impact on Node Clusters

The node clustering (discussed previously in Sec. V-A, and shown in Fig. 4) gives a perspective on the real-world impact a jammer can have on different node clusters. In the real world, wireless jammers only impact the areas in which they are deployed. However, depending on the signal strength, surrounding areas can be affected as well. In this experiment, we deploy *eSWORD* in the Colosseum scenario (shown in Fig. 4) and evaluate how the jammer works in the emulated environment.

Fig. 7 shows the SINR and link status for two nodes belonging to different clusters of the network. The node on the left of the figure belongs to the same group as the jammer; the one on the right is close to the jammer but does not belong to the same cluster. Looking at the node in the same cluster of the jammer (left), we notice that the jammer impact is almost immediate. Indeed, once the jammer is started, the legitimate node can no longer communicate with the other nodes of the network. We also note that the SINR of this node assumes values lower than 0 at times, meaning that the strength of the jamming signal is stronger than that of the legitimate signals received.

Conversely, the node in the different cluster (on the right in the figure) experiences a less severe signal degradation and

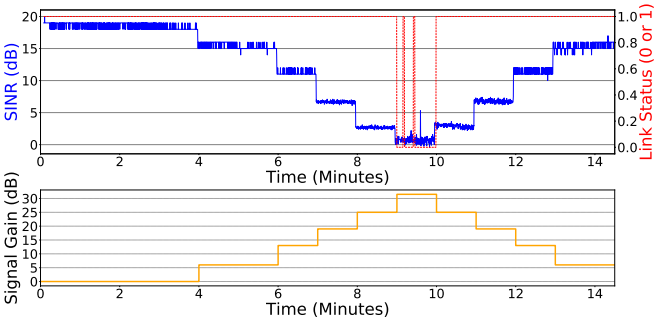

Fig. 6: Top: impact a jammer has on a node's link status and SINR based on the gain of the signal over time. Bottom: the jammer's change in gain over time, showing how the SINR of a node and the signal gain mirror each other.

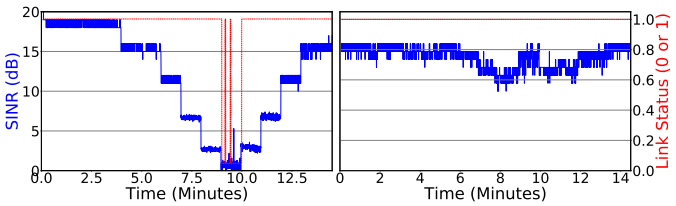

Fig. 7: Two nodes where one (left) is in the same group as the jammer and the other node (right) is relatively close, but not in the same group.

can communicate throughout the experiment. This is due to the fact that even though we notice several instants in which the SINR of the node decreases (e.g., at minutes 7 to 9, and 14-15), meaning that the jammer can reach nodes further away, it does so with limited signal strength that does not interrupt the ongoing communications. Overall, we observe that the node in the different cluster (which is further away from it) only experiences a SINR degradation up to 38%, while the node in the same cluster (closer to the jammer) experiences a SINR drop up to 70%, and in multiple instants of the experiment.

These experiments demonstrate that the *eSWORD* prototype implemented on the Colosseum wireless network emulator allows us to perform realistic experiments in a controlled environment. Concerning the location of the critical infrastructure, *eSWORD* allows users to not only jam nodes in close proximity to the jammer, but also those further away. This reflects on the deployment of real-world network nodes and components, which may not be confined to a single location, but may be across different ones. Adversaries can exploit this knowledge to aim to take out specific portions of the infrastructure, and potentially cripple the entire network. By enabling the testing of jamming attacks in controlled but realistic environments, *eSWORD* allows users to evaluate the resilience of such critical network systems without harming commercial infrastructures, and to find robust ways to counter such forms of attack.

VII. Conclusion

In this paper, we introduced *eSWORD*, a novel framework that allows for accurate, large-scale jamming attack experimentation with HITL in a controlled environment. We prototyped *eSWORD* on the Colosseum wireless network emulator and demonstrated its capabilities on a large-scale network with 49 cellular nodes deployed on realistic urban wireless scenarios. Finally, we verified the accuracy of *eSWORD* results by comparing them with those obtained in an over-the-air wireless testbed. *eSWORD*'s capabilities, scale, and controlled experimentation are key in advancing jamming research, for instance, to devise techniques to counter jamming attacks and to evaluate network resilience to them, which future works will focus on.

References

[1] "Electronic Warfare," Aug. 2020. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare.html

[2] "Electronic Warfare Market." [Online]. Available: https://www.marketsandmarkets.com/

[3] K. Grover, A. Lim, and Q. Yang, "Jamming and anti-jamming techniques in wireless networks: A survey," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, 2014.

[4] O. Puñal, I. Aktas, C.-J. Schnelke, G. Abidin, K. Wehrle, and J. Gross, "Machine Learning-based Jamming Detection for IEEE 802.11: Design and Experimental Evaluation," Jun. 2014.

[5] B. Upadhyaya, S. Sun, and B. Sikdar, "Machine Learning-based Jamming Detection in Wireless IoT Networks," in *2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS)*, Aug. 2019, pp. 1–5.

[6] S. Gecgel, C. Goztepe, and G. K. Kurt, "Jammer Detection based on Artificial Neural Networks: A Measurement Study," in *WiseML*, ser. WiseML 2019. New York, NY, USA: Association for Computing Machinery, May 2019, pp. 43–48.

[7] J. Kanwar, N. Finne, N. Tsiftes, J. Eriksson, T. Voigt, Z. He, C. Åhlund, and S. Saguna, "JamSense: Interference and Jamming Classification for Low-power Wireless Networks," in *2021 13th IFIP WMNC*, Oct. 2021.

[8] Y. Arjoune, F. Salahdine, M. S. Islam, E. Ghribi, and N. Kaabouch, "A Novel Jamming Attacks Detection Approach Based on Machine Learning for Wireless Communication," in *2020 International Conference on Information Networking (ICOIN)*, Jan. 2020, pp. 459–464.

[9] "Jammer Enforcement," Mar. 2011. [Online]. Available: https://www.fcc.gov/general/jammer-enforcement

[10] L. Bonati, P. Johari, M. Polese, S. D'Oro, S. Mohanti, M. Tehrani-Moayyed, D. Villa, S. Shrivastava, C. Tassie, K. Yoder, A. Bagga, P. Patel, V. Petkov, M. Seltser, F. Restuccia, A. Gosain, K. R. Chowdhury, S. Basagni, and T. Melodia, "Colosseum: Large-Scale Wireless Experimentation Through Hardware-in-the-Loop Network Emulation," in *DySPAN*, Virtual Conference, December 2021.

[11] A. Benslimane, A. yakoubi, and M. Bouhorma, "Analysis of Jamming Effects on IEEE 802.11 Wireless Networks," Jul. 2011, pp. 1–5.

[12] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: reactive jamming in wireless networks: how realistic is the threat?" in *Proceedings of ACM conference on Wireless Network Security*, New York, NY, USA, June 2011.

[13] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing*, New York, NY, USA, May 2005, pp. 46–57.

[14] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks," in *Proceedings of IEEE INFOCOM*, May 2007.

[15] S. Vadlamani, B. Eksioglu, H. Medal, and A. Nandi, "Jamming attacks on wireless networks: A taxonomic survey," *International Journal of Production Economics*, vol. 172, pp. 76–94, Feb. 2016.

[16] A. Proaño and L. Lazos, "Selective Jamming Attacks in Wireless Networks," in *2010 IEEE International Conference on Communications*, May 2010, pp. 1–6.

[17] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," *IEEE Pervasive Computing*, vol. 7, no. 1, pp. 74–81, Jan. 2008.

[18] H. Pirayesh and H. Zeng, "Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 2, pp. 767–809, 2022.

[19] M. Çakıroğlu and A. Özcerit, *Jamming Detection Mechanisms for Wireless Sensor Networks*, Jun. 2008.

[20] N. Aschenbruck, E. Gerhards-Padilla, and P. Martini, "Simulative Evaluation of Adaptive Jamming Detection in Wireless Multi-hop Networks," in *2010 IEEE 30th International Conference on Distributed Computing Systems Workshops*, Jun. 2010, pp. 213–220.

[21] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[22] K. Dostert, "Frequency-hopping spread-spectrum modulation for digital communications over electrical power lines," *IEEE Journal on Selected Areas in Communications*, vol. 8, no. 4, pp. 700–710, 1990.

[23] U. Madhow and M. Honig, "MMSE interference suppression for direct-sequence spread-spectrum CDMA," *IEEE Transactions on Communications*, vol. 42, no. 12, pp. 3178–3188, 1994.

[24] M. T. Thurbon, "The Origins of Electronic Warfare," *The RUSI Journal*, vol. 122, no. 3, pp. 56–63, Sep. 1977.

[25] "MITRE | Solving Problems for Safer World." [Online]. Available: https://www.mitre.org

[26] L. Bonati, S. D'Oro, S. Basagni, and T. Melodia, "SCOPE: An Open and Softwarized Prototyping Platform for NextG Systems," in *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*. Virtual Event, WI: ACM, 2021.

[27] L. Bertizzolo, L. Bonati, E. Demirors, A. Al-shawabka, S. D'Oro, F. Restuccia, and T. Melodia, "Arena: A 64-antenna SDR-based Ceiling Grid Testing Platform for Sub-6 GHz 5G-and-Beyond Radio Spectrum Research," *Computer Networks*, vol. 181, pp. 1–17, 2020.