Deep Learning Dataset Generation for Physical Layer Authentication in Wireless Sensor Networks (WSN)

Christopher Dentremont
Department of Electrical and Computer Engineering
Univesity of Massachusetts Dartmouth
North Dartmouth, USA
CDentremont1@UMassD.edu

Hong Liu
Department of Electrical and Computer Engineering
Univesity of Massachusetts Dartmouth
North Dartmouth, USA
HLiu@UMassD.edu

***Abstract*— Structural Health Monitoring (SHM) uses wireless sensor network (WSN) to monitor a civil construction's conditions remotely and constantly for its sustainable usage. Security in WSN for SHM is essential to safeguard critical transportation infrastructure such as bridges. While WSN offers cost-effective solutions for Bridge SHM, its wireless nature expands attack surfaces, making security a significant concern. Despite progress in addressing security issues in WSN for Bridge SHM, challenges persist in device authentication due to the unique placement of sensor nodes and their resource constraints, particularly in energy conservation requirements to extend the system's lifetime. To overcome these limitations, this paper proposes an innovative authentication scheme with deep learning at the physical layer. Our approach steers away from conventional device authentication methods: no challenge-response protocol with heavy communication overhead and no cryptography of intensive computation. Instead, we use radio frequency (RF) fingerprinting to authenticate sensor nodes. Deep learning is chosen for its ability to discover patterns in large datasets without manual feature engineering. We model our scheme on IEEE 802.11ah, Wi-Fi HaLow of long-range communication and low-power consumption for machine-to-machine (M2M) applications. Simulations and experiments using universal software radio peripheral (USRP) demonstrate the effectiveness of the proposed scheme. By integrating security into Cyber-Physical System/the Internet-of-Things (CPS/IoT) design of WSN for Bridge SHM, our work contributes to critical infrastructure protection.**

Keywords—wireless sensor network (WSN), transceiver design, bridge structural health monitoring (SHM), deep learning for physical layer security, fingerprinting, machine learning for resource management

I. INTRODUCTION

Ensuring the security of Wireless Sensor Network (WSN) used for Bridge Structural Health Monitoring (SHM) has emerged due to economic and safety consequences associated with protecting the nation's critical infrastructure [1]. Bridge SHM, a process that determines and tracks the structural integrity of bridges, observes the physical world where civil, mechanical, and electrical engineers identify and characterize potential damage, corrosion, and other structural responses to forcing events. WSN, connecting autonomous data acquisition nodes which each encompasses sensing elements, multiprocessor with memory, and wireless communication components, creates a cyber space in the computer science and engineering realm. Sensors/transducers link the physical world and the cyber space by converting variations in a physical quantity to data streams in an electrical signal. In the context of Bridge SHM, sensors include strain gauges, load cells, accelerometers, and inclinometers. Therefore, WSN-based Bridge SHM is a type of cyber-physical system (CPS) [2].

Over the past two decades, significant progress has been made in the development of WSN for Bridge SHM. Wisden, an early work in 2004, demonstrated a transition from wired sensing to wireless by designing a WSN prototype software system that reliably delivered time-synchronized structural-response data from multiple locations to a central server [3]. The deployment of a WSN-based SHM system on the Golden Gate Bridge (GGB) in 2007 marked a significant milestone [4]. Further advancements focused on machine learning techniques for bridge rating and in-network processing to optimize energy consumption and extend the system's lifetime [5].

Despite these achievements, security concerns within WSN for Bridge SHM have been a longstanding issue. WSN presents a double-edged sword, offering cost-effective solutions for SHM while exposing vulnerabilities to potential cyber-attacks. The massive dense deployment of sensor nodes poses challenges in device authentication, and the resource constraints of sensor nodes render conventional security methods ineffective [6]. Although some remedies leverage WSN features such as random, grid, or cluster configurations [7], the specific requirements of Bridge SHM, which necessitate node placement at critical locations for accurate damage detection, demand innovative security mechanisms. Presently, research in WSN for SHM predominantly focuses on performance metrics such as sensing coverage, communication range, energy consumption, reliability, and lifetime, neglecting the crucial aspect of security. Drawing lessons from the early days of the Internet, it is imperative to incorporate security into the design of WSN for Bridge SHM in particular and CPS in general, rather than relying on post-deployment patching.

This paper addresses the aforementioned security challenges by proposing an innovative authentication scheme that employs

This work was supported in part by the National Science Foundation (NSF) Innovations in Graduate Education (IGE) program under grant #2105718 Graduate Education in Cyber-Physical Systems Engineering.

deep learning at the physical layer focusing on generating datasets for such a scheme. To save communication overhead, our scheme involves no challenge-response protocol during authentication process. Furthermore, we leverage radio frequency (RF) fingerprinting, instead of computationally intensive cryptography such as digital signature to verify the source of a message [8]. We choose deep learning in authenticating sensor nodes to a data logger, for the need of agility in the unpredictable arms race of WSN security. Deep learning can discover patterns in large datasets without the need of manual feature engineering [7]. WSN for Bridge SHM readily collects or arguments massive datasets. We demonstrate our approach's security effectiveness on IEEE 802.11ah (aka Wi-Fi HaLow), a wireless networking standard for machine-to-machine (M2M) and Internet-of-Things (IoT) applications [9], the core of CPS. Results from simulations in MATLAB and experiments with Software Defined Radio (SDR) demonstrate the effectiveness of our approach. The main contributions of our work are as follows:

- Devise an innovative physical-layer authentication scheme, leveraged by deep learning, suitable to ensure source integrity in WSN for Bridge SHM.
- Address the limitations of existing security mechanisms in critical infrastructure protection to ensure the safety and performance of CPS, particularly of Bridge SHM.
- Demonstrate feature extraction of RF fingerprinting for building deep learning datasets used for physical layer authentication.
- Add security in CPS designs, applicable to protect other critical infrastructures with similar characteristics such as tunnels in transportation, powerlines in energy, and borders in homeland.

II. WSN Security Requirements and Attack Model

A. System Architecture

We adopt CPS design principles in developing the system architecture of WSN for Bridge SHM. The trend of deploying WSN for SHM towards CPS design is anticipated to alleviate WSN resource constraints and effectively meet the specific requirements of SHM applications, by multidisciplinary collaborations among engineering and computing. However, comprehensive CPS design remains an open issue [2]. Integrating security in CPS design is challenging.

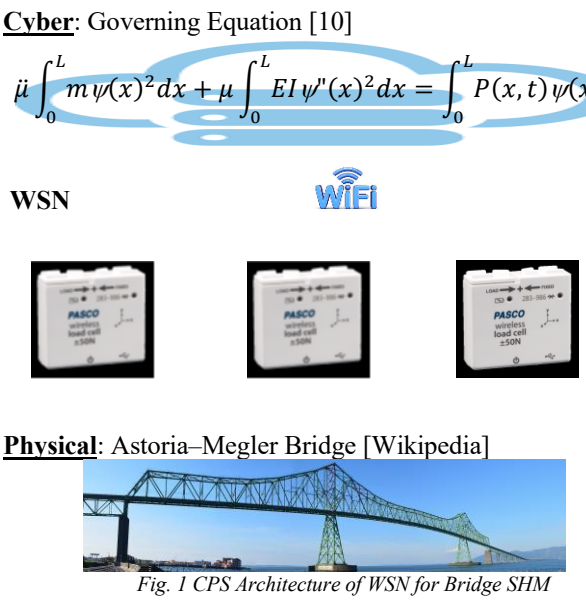

Fig. 1 CPS Architecture of WSN for Bridge SHM

Fig. 1 illustrates our CPS architecture of WSN for Bridge SHM. A physical world contains a bridge with its substructures of physical elements. Civil, mechanical, and electrical engineers examine the physical aspects of the bridge such as its response to environmental forces for crack event detection. A cyber space models the bridge dynamics, such as the governing equation for a beam's vertical dynamic displacement $\mu(x,t)$, i.e. vibration, of a single-degree-of-freedom beam on a truss bridge with span L, mass m, shape function $\psi(.)$, flexural rigidity EI, and time-variant load $P(.)$ [10].

Sensors in WSN, such as the load cells made by PASCO, measure tension and compression forces in a bridge. Sensors provide the perspective of a physical world to a cyber space for detection, replacing costly and risky manual inspection. The amount of raw data collected is small, in hundreds to a few thousand bytes. For Bridge SHM, a part of a bridge, called *substructure*, can be monitored independently without the need to examine the whole structure. Thus, a group of *sensor nodes* (each with sensing, processing/storage, and communication components), called *subnetwork*, is placed on a substructure. Sensor nodes are battery-operated to save cabling hassles as in wired sensor network and to save investment cost as in energy-harvesting devices. Most wireless sensor platforms are supplied with limited power. For example, Crossbow MICAz has two AA batteries, lasting several weeks while Intel Imote2 has two AAA batteries, up to a few months. Resources are also limited in sensor nodes. MICAz has ATmega128L (8-bit, 16MHz) CPU, 128KB ROM for code and 4KB RAM for data [2].

Adopting CPS design principles, engineering and computing experts co-design the SHM system to optimize both WSN performance (network lifetime) and application performance (damage detection) [11]. Each aspect involves different but intertwined issues: cyber builds a computation model from data collected and information exchanged by computer scientists/engineers while physical dynamics of a bridge are studied by civil, mechanical, and electrical engineers. More particularly in Bridge SHM, our previous work demonstrated the achievement by engineering and computing collaboration in time domain responses for Bridge SHM, which otherwise had resulted in suboptimal solutions if cyber and physical aspects are processed separately [12].

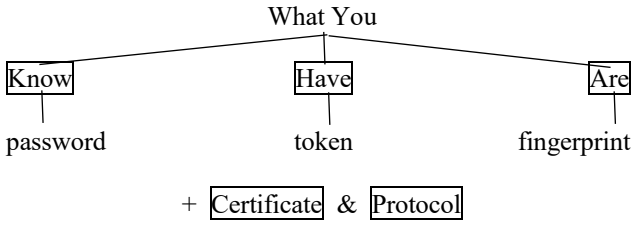

Fig. 2 Device Authentication

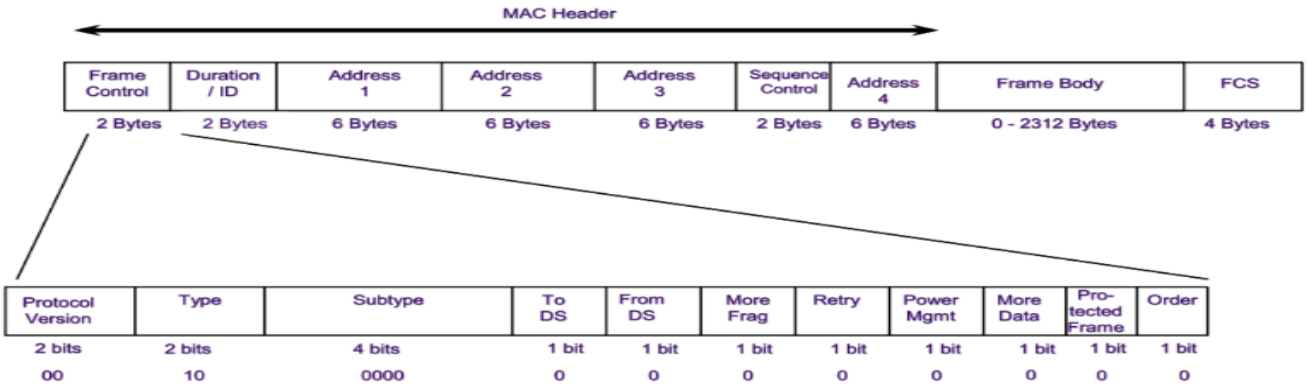

Fig. 3 IEEE 802.11 Frame Format

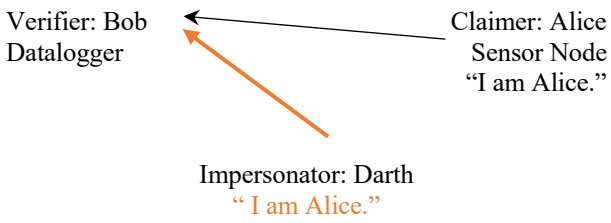

Fig. 4 Attack Model against Device Integrity

a) B. WSN Security Requirements for Bridge SHM

Security services aim at three general goals: Confidentiality, Integrity, and Availability, abbreviated as *C.I.A*. *Confidentiality* prevents data from unauthorized access. *Integrity* is divided into two categories: one is Data Integrity that protects data in transmission or at storage from unauthorized changes or fabrication; the other is Device Integrity, also known as Source Integrity, to assure that a device or system is not compromised or tampered. *Availability* ensures that legitimate users can access resources (system, data, and service) without disruption.

CPS/IoT exposes layers of attack surfaces [7]:

- *Perception Layer:* where sensors collect data including the medium that they use to communicate. Physical tampering and resource depletion
- *Network Layer:* where transceivers (Tx/Rx) deliver data to access points (AP) for datalogger/server
- *Application Layer:* where a server processes data based on some computation model to make intelligent decisions[7].

Device Integrity defends the frontline of WSN for Bridge SHM. As shown in *Fig. 2*, device integrity is classified into three levels by the answering the questions of:

2) *What You Know? For example,* password.
3) *What You Have? For example,* token or smart card.
4) *What You Are? For example,* fingerprint.

These schemes are enhanced by cryptography-based certificates and challenge-response protocols.

C. Attack Model

In the context of WSN for Bridge SHM, one-way authentication by sensor nodes to the datalogger is sufficient. *4* illustrates the attack scenario where "Alice" is one of the sensor nodes in the network collecting data. The datalogger "Bob" will authenticate Alice as a device in the network before retrieving its data through the wireless channel. The impersonator "Darth" aims to gain the trust of Bob by authenticating itself under the guise of Alice. If successful, Darth is able to transmit fabricated data freely to Bob and Bob will present it as collected data from a trusted node.

III. VULENRABILITY ANALYSIS OF IEEE 802.11AH

A. IEEE 802.11ah for Bridge SHM

With low-power consumption and long-range coverage, IEEE 802.11ah is an ideal wireless communication standard suitable to WSN for Bridge SHM [13]. Sub 1 GHz operating frequency reduces attenuation when propagating through surfaces. This addresses the concerns involving the deployment of our WSN for Bridge SHM where sensor nodes are required to communicate through dense material. IEEE 802.11ah Medium Access Control (MAC) allows for shared communication to more Access Points (APs) in the sensor network. 802.11ah stations are not required to be always on by eliminating Traffic Information Message (TIM) in the data frame. Non-TIM stations reduce power consumption in M2M and IoT applications [9].

The data frame format remains the same across the family of IEEE 802.11 standards, shown in *Fig. 3*.

- Frame Body field stores the payload received from a higher layer. It can vary in length but has a maximum size of 2312 octets.
- Frame Check Sequence (FCS) field is responsible for error detection in the received frame.
- Frame Control Field includes bits used to indicate the version of the IEEE 802.11 MAC and the Protected Frame bit.

- Duration field allows a station (STA) to determine the remaining duration of the frame exchange between the station and the AP.
- Sequence Control field assists the STA in identifying duplicate frames and helps in reassembling fragmented frames.
- The MAC header of a data frame includes four separate address fields, although not all of them contain relevant addresses in every case. These address fields identify the original source address (SA), final destination address (DA), receiver address (RA), and either the transmitter address (TA) or the BSS identifier (BSSID), depending on the function of the frame.

B. Threats to IEEE 802.11ah

IEEE 802.11ah shares the same frame format and protocols as other standards in IEEE 802.11 making it susceptible to some of the same attack threats. Common attacks to device integrity in CPS/IoT and M2M applications include 1) spoofing and 2) replay attacks[14].

1) Spoofing: Attackers attempt to replicate a trusted device in the network to steal or manipulate data after gaining accesss.

2) Replay Attack: Data is intercepted during transmission by an attacker and used to gain access by resending the captured data to trick the recipient to accept the transmission as legitimate.

Attacks are carried out by exploiting vulnerabilities in the component's software/hardware in the network. The National Vulnerabilities Database (NVD) labels and makes known these Critical Vulnerabilities and Exposures (CVEs) identified by trusted authorities. Mapping CVEs using language models identify present threats in a network that leave openings for attack [6]. Link predictions and text-to-text models can associate known vulnerabilities to infer potential risks in software based on test generation. Good security management for WSNs must include awareness of known vulnerabilities and exposures paired with a plan to identify their presence and eliminated attackers ability to exploit them.

IV. Defend with Deep Learning

A. Deep Learning in CPS/IoT Security

Deep Learning (DL) offers several benefits for remote WLANs. Deep learning can take large data sets and extract complex patterns through neural networks. The ability to automate the deep learning process makes it a better choice in our system compared to Machine Learning (ML) which requires more processing power and feature engineering [15]. This research focuses on dataset generation for two types of deep neural networks 1) Convolutional Neural Network, 2) Reinforcement Learning. The training is to be performed offline while the testing is online.

1) Convolutional Neural Network (CNN): Reduces layer connections in neural network decresing computation requirements while also maintaining high performance. *Fig. 5* is

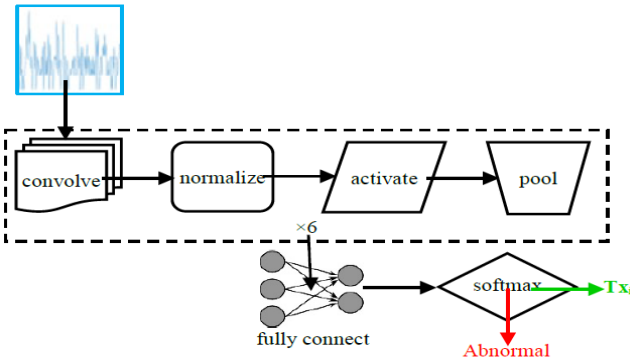

Fig. 3 CNN-Rx Architecture [8]

a successful example of Rx uses CNN model to classify legitimate Tx's and abnormal ones [8].

2) Reinforcement Learning (RL): Produces output solution through trial and error with success in spoofing attack protection.

B. Deep Learning to Device Integrate in WSN for SHM

Deep learning, data-driven by RF fingerprinting, can be a powerful security tool for device authentication of sensor nodes in the WSN for Bridge SHM [8]. RF fingerprints can be used to characterize wireless transmissions in a WSN where a deep learning network can identify malicious channels.

Physical characteristics of the sensor node, such as Rx and Tx integrated circuit, contain process imperfections from manufacturing. These imperfections contribute to the RF fingerprint of devices giving them a Physical Unclonable Function (PUF) which cannot be falsely mapped. By building a dataset of extracted Rx/Tx specific features, we can label known devices and authenticate them through the DL network.

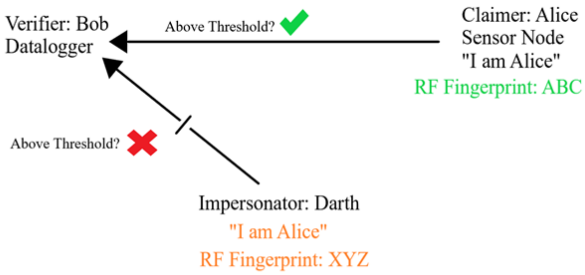

Fig 6. Attack Model with DL Solution Implemented

The dataset is compiled through feature extraction for legitimate sensor node's unique RF signatures. This is established through features such as signal strength, phase noise, frequency offset, and modulation characteristics depending on the node and WSN. A supervised CNN model is trained and labeled with legitimate and malicious transmitters. This scheme defends the WSN from the attack model in *Fig. 3* adding a layer of authentication for the datalogger that an attacker cannot impersonate.

Fig. Depicts the attack model with DL implemented at the physical layer of the datalogger. Darth attempts to pose as Alice but is unsuccessful after the DL model identifies it does not meet the threshold set by the RF fingerprint.

V. EVAULATION

The testing setup depicted in *Fig. 7* shows the WLAN using four Raspberry Pi ™ Model 4 units with the AHPI7292S HAT form factor developed by ALFA Network Inc. This attachment allows 802.11ah communication between the Raspberry Pi boards where one is setup as an AP and the other three are STAs (A, B & C). Signals are captured on the ADALM-PLUTO software defined radio module and can be processed using MATLAB signal processing software as shown in *Fig. 8*. Each device in the WSN

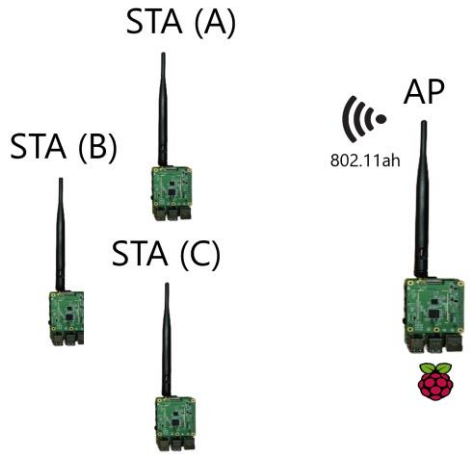

Fig. 7 IEEE 802.11ah with-Deep Learning Testing Setup

that employs our scheme must be captured and input into the dataset so the AP can recognize it. The captured signal undergoes feature extraction using techniques such as the spectral analysis in *Fig. 9* performed on STA A. Analyzing the features of the

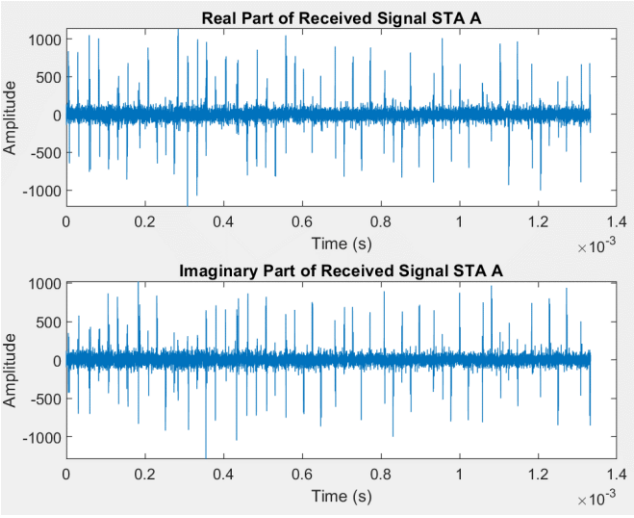

Fig. 8 Captured Signal from STA A

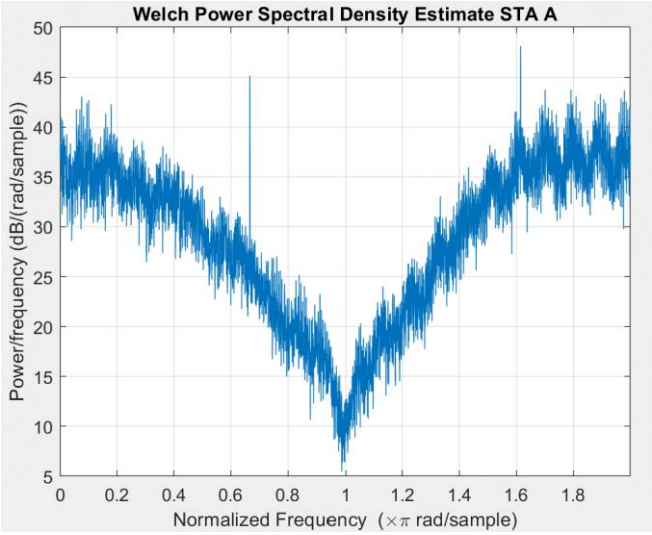

Fig. 9 Spectral Analysis of Captured Signal from STA A

signal allow us to build a deep learning dataset that can differentiate between signals originating from trusted devices or masquerading nodes. By training the AP before the WSN is deployed we can authenticate nodes at the PHY layer and create a framework deep learning dataset generation that can be adapted to many WSN applications beyond Bridge SHM. The effectiveness of this scheme can be measured using network security measurement indicators such incident detection ability [19].

VI. CONCLUSION AND FUTURE WORK

WSN has become crucial for Bridge SHM to ensure safe operation of the nation's critical infrastructure. However, WSN security remains a significant concern due to potential economic and safety consequences. Although progress has been made to address the security issues in WSN for Bridge SHM, the peculiar placement of sensor nodes and their resource constraints, especially in the need to conserve energy consumption, pose challenges in device authentication.

To overcome these limitations, we propose an innovative authentication scheme of sensor nodes that utilizes deep learning at the physical layer and provides a framework for generating datasets for this scheme. Our approach saves communication overhead by skipping challenge-response protocol. Utilizing RF fingerprinting, instead of cryptography-based authentication methods, reduces computation cost. Deep learning is chosen for its ability to discover patterns in large datasets without manual feature engineering. The effectiveness of our scheme is demonstrated on IEEE 802.11ah through simulations in MATLAB and experiments with Software Defined Radio (SDR) By incorporating security into the design of WSN for Bridge SHM, our work contributes to the protection of critical transportation infrastructure.

Future work includes systematic testing of our proposed scheme for device authentication. Using generative adversarial network (GAN), we examine the limit of our scheme to discriminate legitimate devices from spoofed instances that

another deep learning model generates. We will extend our physical-layer authentication scheme to two-way authentication between sensor nodes and data loggers as well as prevention of sybil attacks among many threats to WSN for Bridge SHM.

ACKNOWLEDGMENT

The authors thank Honggang Wang of UMass Dartmouth and Tzuyang Yu of UMass Lowell for their support throughout this research. Gratitude also goes to Trina Kershaw of UMass Dartmouth, Susan Tripathy and Kavitha Chandra of UMass Lowell for their critics.

REFERENCES

[1] D. Egan, C. Nelson, F. Roberts, A. Rose, A. Tucci, and R. Whytlaw, "Complex Economic Consequence Analysis to Protect the Maritime Infrastructure," in *2022 IEEE International Symposium on Technologies for Homeland Security, HST 2022*, IEEE, 2022. doi: 10.1109/HST56032.2022.10024979.

[2] Z. A. M. Bhuiyan, J. Wu, G. Wang, J. Cao, W. Jiang, and M. Atiquzzaman, "Towards cyber-physical systems design for structural health monitoring: Hurdles and opportunities," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 4, 2017, doi: 10.1145/3086508.

[3] N. Xu, K. K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A Wireless Sensor Network For Structural Monitoring," in *2nd international conference on Embedded networked sensor systems (SenSys)*, ACM, 2004, pp. 13–24. doi: 10.1145/1031495.1031498.

[4] S. Kim *et al.*, "Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks," in *Sixth International Symposium on Information Processing in Sensor Networks (IPSN)*, IEEE, 2007, pp. 254–263. doi: 10.1109/IPSN.2007.4379685.

[5] S. A. Putra, B. R. Trilaksono, M. Riyansyah, D. S. Laila, A. Harsoyo, and A. I. Kistijantoro, "Intelligent sensing in multiagent-based wireless sensor network for bridge condition monitoring system," *IEEE Internet Things J*, vol. 6, no. 3, pp. 5397–5410, Jun. 2019, doi: 10.1109/JIOT.2019.2901796.

[6] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2. pp. 2–22, Jun. 2006. doi: 10.1109/COMST.2006.315852.

[7] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1646–1685, Jul. 2020, doi: 10.1109/COMST.2020.2988293.

[8] J. Lu, T. Morehouse, J. Yuan, and R. Zhou, "Machine-Learning PUF-based Detection of RF Anomalies in a Cluttered RF Environment," in *2021 IEEE Virtual IEEE International Symposium on Technologies for Homeland Security, HST 2021*, IEEE, 2021. doi: 10.1109/HST53381.2021.9619834.

[9] Y. Zhou, H. Wang, S. Zheng, and Z. Z. Lei, "Advances in IEEE 802.11ah Standardization for Machine-Type Communications in Sub-1GHz WLAN," in *IEEE International Conference on Communications (ICC) - 2nd Workshops on Telecommunication Standards: From Research to Standards*, IEEE, 2013.

[10] R. Batchu, K. Raisi, and T. Yu, "Structural Health Monitoring of a Train Model under Traffic Loading," in *SPIE Smart Structures + Nondestructive Evaluation conferences*, SPIE, Mar. 2023. [Online]. Available: http://SPIE.org/manuscripts

[11] G. Hackmann, W. Guo, G. Yan, Z. Sun, C. Lu, and S. Dyke, "Cyber-physical codesign of distributed structural health monitoring with wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 63–72, Jan. 2014, doi: 10.1109/TPDS.2013.30.

[12] T.-Y. Yu, H. Wang, and H. Liu, "Denoising of Time Domain Responses in Wireless Sensor Network for the Structural Health Monitoring of Transportation Infrastructure," in *ACM Proceedings of the 44th Annual Simulation Symposium (ANSS)*, ACM, 2011, pp. 183–187.

[13] J. F. Kurose and K. W. Ross, "Chapter 7 Wireless and Mobile Networks," in *Computer Networking: A Top-Down Approach, 8 th Edition*, Pearson, 2021, pp. 531–577.

[14] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Communications Surveys and Tutorials*, vol. 20, no. 4. IEEE, pp. 3453–3495, Oct. 01, 2018. doi: 10.1109/COMST.2018.2855563.

[15] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 3, pp. 1646–1685, Jul. 2020, doi: 10.1109/COMST.2020.2988293.

[16] K. Cao and L. Zhang, "A Novel Method of Network Security Measurement Based on Indicators," in *2023 International Wireless Communications and Mobile Computing, IWCMC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 877–883. doi: 10.1109/IWCMC58020.2023.10183184.