Software-Defined Cyber–Energy Secure Underwater Wireless Power Transfer

Jiangwei Wang, *Student Member, IEEE*, Yanyuan Qin, *Student Member, IEEE*, Zefan Tang, *Student Member, IEEE*, and Peng Zhang, *Senior Member, IEEE*

***Abstract*—Underwater wireless power transfer (UWPT) is a critical infrastructure for supplying power to underwater devices, such as underwater sensors and autonomous underwater vehicles. Enabling a software-defined architecture for UWPT promises to build a flexible and programmable underwater energy network. Although it is crucial that UWPT be made more resilient to cyber-attacks and energy stealing, this remains an open challenge. In this article, we propose a software-defined UWPT (SD-UWPT) system that is both cyber and energy secure. A moving target defense approach and an active synchronous detection method are developed to protect the SD-UWPT against scanning-based attacks and power bot attacks. To enable energy-secure UWPT, an impedance measurement based approach is further established to prevent energy stealing. Through comprehensive evaluations, we validate the benefits of SD-UWPT and demonstrate the effectiveness of the proposed cyber–energy secure strategies against various attacks.**

***Index Terms*—Cybersecurity, energy security, software-defined architecture, underwater wireless power transfer (UWPT).**

I. Introduction

DUE TO increased demand from undersea industries, smart ocean systems such as underwater sensor networks, ocean monitoring devices, and autonomous underwater vehicles (AUVs) are more popular than ever [1]. Internet of Things (IoT) would enable a system that different underwater devices can communicate with each other, and transfer data between devices and control center [2]. However, supplying power to these IoT-enabled underwater devices can be difficult. Manually replacing batteries can be time consuming and disruptive, whereas wired power transfer techniques can be associated with corrosion issues and high maintenance costs. Underwater wireless power transfer (UWPT) is the promising technique that addresses all these issues [3], [4]. UWPT is more time efficient and less disruptive than manually replacing batteries, and unlike more expensive wired power transfer techniques, there is no risk of electrode corrosion.

Despite its benefits, UWPT poses some challenges. Using a traditional communication infrastructure for UWPT is hardware dependent, rendering it both costly and inefficient, and the dynamic status changes of UWPT devices make it challenging to flexibly manage those devices. Recently, the software-defined networking (SDN) has been adopted in various networking systems and shown its effectiveness. Software-defined control has been adopted in microgrids [5] to enable a flexible and programmable network environment. SoftWater was proposed for underwater wireless communication networks. It is able to incorporate new underwater communication solutions, accordingly maximizing the network capacity, improving the network robustness, and providing truly differentiated and scalable networking services [6]. In this study, we devise a software-defined UWPT (SD-UWPT) architecture that enables the optimal routing of UWPT communications and the dynamic management of UWPT devices.

Although the SD-UWPT system has a number of benefits, it also has some critical security issues. Specifically, it is vulnerable to both cyberattack and energy stealing. First, the network's visibility and programmability make it prone to cyberattacks [7]. Those cyberattacks can be categorized into two types: One is *the first-generation cyberattack* such as the DoS attack [8]. This kind of attacks can disable the docking stations (docks), which is the critical element in SD-UWPT system for power and data transfer. The other is the emerging *second-generation attack* such as the power bot attack [9]. The power bot attack, which aims at attacking the controller of an AUV, can effectively reduce power efficiency by changing the topology of the controller or by modifying its parameters. Second, the system's vulnerability to energy stealing means that an unauthorized AUV can pretend to be an authorized user and steals energy from the system, disrupting the tasks of authorized AUVs. Therefore, ensuring both cybersecurity and energy security is of great importance for the development of SD-UWPT systems.

There are existing approaches to protect SDN from cyber-attacks, such as model checking with symbolic execution [10], binary decision diagrams [11], and language-based security [12]. Furthermore, cybersecurity has long been a hot topic in underwater wireless network. Typical security threats in underwater

Manuscript received April 20, 2020; revised July 4, 2020 and October 16, 2020; accepted November 15, 2020. Date of publication November 18, 2020; date of current version December 18, 2020. This work was supported in part by the National Science Foundation under Grant ECCS-1831811/2018492, in part by the Office of the Provost, University of Connecticut, and in part by the Office of Naval Research under Award N00014-20-1-2858. *(Corresponding author: Peng Zhang.)*

Jiangwei Wang is with the Department of Electrical and Computer Engineering, University of Connecticut, Storrs, CT 06269 USA (e-mail: jiangwei.wang@uconn.edu).

Yanyuan Qin is with the Department of Computer Science and Engineering, University of Connecticut, Storrs CT 06269 USA (e-mail: yanyuan.qin@uconn.edu).

Zefan Tang and Peng Zhang are with the Department of Electrical and Computer Engineering, Stony Brook University, Stony Brook, NY 11794 USA (e-mail: zefan.tang@stonybrook.edu; p.zhang@stonybrook.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JESTIE.2020.3039107.

Digital Object Identifier 10.1109/JESTIE.2020.3039107

wireless network have been categorized according to different layers, which are as follows:

1) physical layer attacks, including jamming attack[13] and eavesdropping [14];
2) link layer attacks, such as replay attacks and Sybil attacks;
3) network layer attacks, such as routing attacks and packet interception;
4) transport layer attacks [15].

Corresponding countermeasures are proposed to mitigate the security threats. Detection of abnormality[13], game theory, and reinforcement learning based methods [16] are devised to protect and mitigate the system from jamming attacks. State information of the nodes is utilized to detect the Sybil attack with the assumption of availability of beacon nodes [17]. Securing networking protocols, including securing communication channel schemes [18] and attack-resilient routing protocols [19], are proposed to strengthen the system security. Cryptographic primitives, such as symmetric key encryption [20], public key generation and distribution [21] and authentication are also investigated to provide confidentiality and integrity in underwater wireless networks.

However, most of the existing literature focuses on attacks at different networking devices, leaving the vulnerabilities of UWPT systems and possible cyberattacks on SD-UWPT systems underinvestigated. Furthermore, the power bot attack in the SD-UWPT system can neither be detected nor eliminated by existing approaches. Finally, ensuring energy security is still an open challenge in the deployment of UWPT systems. To the best knowledge of the authors, there is no existing work on designing energy security strategies for UWPT systems.

To bridge these gaps, three defense and detection strategies, including moving target defense (MTD), active synchronous detection (ASD), and impedance measurement based approach (IMBA), are devised to protect the SD-UWPT from cyberattacks (scanning based attacks and power bot attack) and energy stealing. In this work, we make the following contributions.

1) An SD-UWPT architecture is proposed to provide high flexibility and programmability for UWPT system.
2) A MTD strategy is presented to defend against scanning-based attacks on the docks in the SD-UWPT system. It secures the communication channels for SD-UWPT.
3) An ASD method is devised to protect AUV controllers from power bot attacks, thus ensuring efficient power transfer between the AUV and the docks.
4) An IMBA is further established to detect unauthorized AUVs that are stealing energy. The energy security of SD-UWPT is thereby guaranteed.

The remainder of this article is organized as follows. Section II discusses the design of the SD-UWPT system. Section III describes the cyber and energy-security strategies. Section IV evaluates the performance of the proposed cyber–energy secure SD-UWPT system, and finally, Section V concludes this article.

II. SD-UWPT Architecture

In this section, we introduce the SD-UWPTs architecture as illustrated in Fig. 1. It consists of an information center, as well as multiple AUVs and docks [22]. To be specific, the docks are composed by buoys, charging stations on ships, and wave energy converters [23], [24], which transfer power to AUVs utilizing wave energy. AUVs run different underwater applications (e.g., oceanographic data collection, scientific ocean sampling, pollution and environmental monitoring, distributed tactical surveillance, and mine reconnaissance), collect data, and send it to docks. After being routed among docks, the data are then forwarded to the information center, which is constituted of a satellite and onshore station. The satellite relays the data between docks and onshore stations. After the data are processed, additional commands from the information center are sent back to the AUVs to perform the tasks. The communication links are represented by the green dashed line in Fig. 1. It is worth noting that the communication can be a combination of different technologies, such as acoustic, optical, and electromagnetic. Acoustic communication can be adopted when the AUVs are far from the docks since optical and electromagnetic waves attenuate fast with the increasing distance in underwater environment. When AUVs are close to docks, optical and electromagnetic waves are preferred for their higher speeds [25]. In terms of power transfer, the AUVs are charged by the docks as shown by the blue lines in Fig. 1.

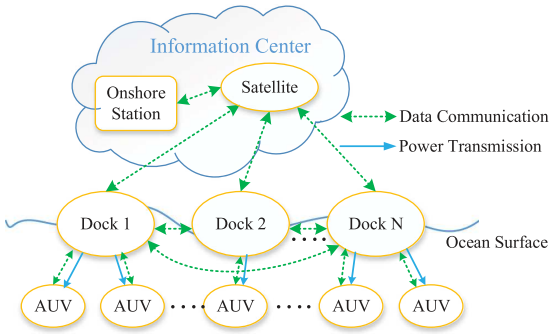


Fig. 1. Architecture of the SD-UWPT system.

Analogous to the SDNs architecture, the information center hosts the network controller, the docks are the nests for the OpenFlow switches and hosts, and the AUVs are the programs running on the host. The benefits of the SD-UWPT architecture include the following.

1) Optimal routing for the communication between AUVs and the information center. The optimal routing in underwater wireless networks has long been shown crucial in minimizing the communication latency [26]–[28]. In UWPT systems, it is critical when some urgent and important tasks need to be carried out by AUVs. When an AUV sends data to a dock, the dock sends a request to the information center to start the data transmission. With the view of the whole traffic of the system, namely the global routing paths of the system, the information center is capable of selecting the optimal routing for each AUV to achieve the maximum throughput.
2) Dynamic structural adjustment. The harsh aquatic environment (e.g., with fouling and corrosion) and the risk of cyberattacks can cause docks to be dysfunctional

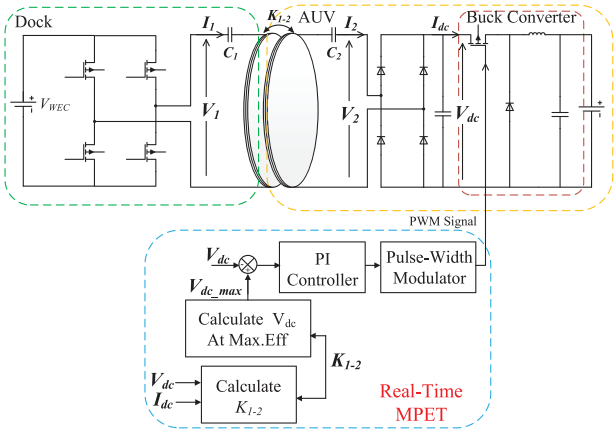


Fig. 2. Circuit topology of one-to-one UWPT.

[29]–[32], which will disable the routing paths associated with those docks, thus disrupting system normal operations. With the advantage of the SDN controller and OpenFlow-based switches, the docks' original flow tables will be updated within the SDN controller to form new routing paths without going through those disabled docks. Furthermore, for the AUVs to be charged by the docks, if a dock does not have sufficient energy for the AUVs, with a global view of the residual energy of the docks, the SDN controller can find another dock to charge the AUVs with the shortest path.

For efficient power transfer, this work adopts the maximum power efficiency tracking (MPET) control [33]. Fig. 2 shows the circuit topology of a one-to-one UWPT system with the MPET control. The input power on the transmitter side is denoted as

$$P_1 = V_1 \cdot I_1 \tag{1}$$

while the output power on the receiver side is

$$P_2 = V_2 \cdot I_2 \tag{2}$$

where V_1, V_2 and I_1, I_2 refer to the voltages and currents for the transmitter and receiver coils, respectively. The efficiency of the coupling coils can be obtained as follows:

$$\eta = \frac{P_2}{P_1} = \frac{w^2 M^2 Z_L}{((Z_L + R_2)R_1 + w^2 M^2)(Z_L + R_2)} \tag{3}$$

where R_1 and R_2 represent the transmitter and receiver coils' resistance, respectively, M is the mutual inductance between the transmitter and receiver coils, and Z_L is the load impedance. ω is the resonant frequency

$$\omega = \frac{1}{\sqrt{L_1 C_1}} = \frac{1}{\sqrt{L_2 C_2}} \tag{4}$$

where L_1, L_2, and C_1, C_2 represent coil inductance and resonant capacitance of the coupling coils, respectively. As the distance between two coils frequently varies due to the dynamic underwater environment, the mutual inductance keeps changes. To maintain a relatively high power efficiency, the reference voltage has to be adjusted according to the varying mutual inductance. The MPET control estimates the coupling coefficient using the secondary voltage and current, and provides the reference voltage for the maximum power efficiency. In the MPET control topology, a machine learning block is utilized to parameterize the secondary voltage and current and estimate the coupling coefficient between the transmitting and the receiving coil [33] as follows:

$$K_{1-2} = \frac{V_1 \pm \sqrt{V_1^2 - 4(V_2 + I_2 R_2) I_2 R_1}}{2 I_2 w \sqrt{L_1 L_2}}. \tag{5}$$

After the coupling coefficient is obtained, the reference secondary voltage can be generated as the input to the PI controller, and the reference voltage for the secondary side can be written as

$$V_{2\max} = V_1 \frac{w K_{1-2} \sqrt{L_1 L_2} \sqrt{\frac{R_1}{R_2}}}{\sqrt{R_1 R_2} + \sqrt{R_1 R_2 + (w K_{1-2})^2 L_1 L_2}}. \tag{6}$$

III. Cyber–Energy Security in SD-UWPT

The SD-UWPT system is vulnerable to cyberattacks and energy stealing. Important tasks carried out by AUVs, including oceanographic data collection, scientific ocean sampling, pollution and environmental monitoring, distributed tactical surveillance, and mine reconnaissance, can be interrupted due to cyberattacks and energy stealing. As the communication channels are necessary, there is no way to exclude the communication between AUVs and docks (or the information center) to avoid cyberattacks and energy stealing. Instead, we need to protect the system from cyberattacks and energy stealing. MTD and ASD strategies are proposed in series to ensure the cybersecurity of the system. The IMBA is further devised to protect the authorized AUVs from energy stealing.

A. MTD on Docks Against Cyberattacks

This article focuses on defending against wormhole attacks because these are among the most devastating cyberattacks faced by underwater wireless communication networks [31], [34]. A wormhole attack is a typical DoS attack in the network layer. A wormhole, namely an out-of-band connection with a higher bandwidth and lower delay, can be created by an adversary between two physical locations in the network. This connection can be radio link created above sea level with fairly fast propagation speed compared with the links in the aquatic environment. Thus, two nodes, namely two docks with long distance, can send packets through the wormhole links since the routing can be the optimal one from their point of view. The traffic can be monitored, and important packets can be dropped or delayed by the wormhole link.

The wormhole attack, however, needs to scan the networks remotely and identify the active hosts as their targets. We propose a MTD [35] to protect the SD-UWPT from the scanning-based attack. Fig. 3 shows the MTD strategy. Benefiting from the software-defined architecture of the whole system, the information center, which acts as a central management authority, coordinates the IP mutation of the whole network. To be specific, a virtual IP address is assigned to each dock by the information center with high unpredictability and mutation speed, whereas

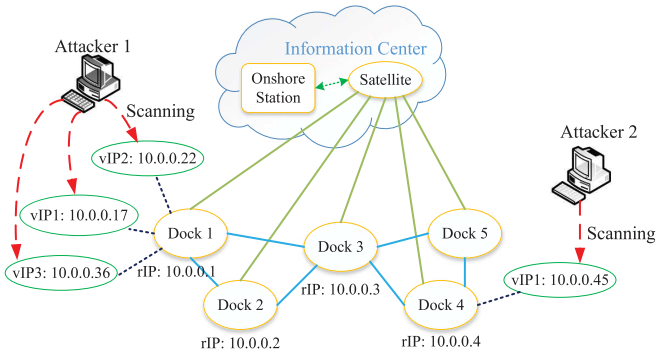


Fig. 3. MTD strategy for the SD-UWPT system.

the real IP address of the dock remains unchanged. Thus, the IP mutation is transparent to the docks. With this specific MTD technique, the docks are reachable via their virtual IP addresses, meanwhile their real IP addresses can only be reached by authorized entities, namely the information center. Therefore, the target IP address that the adversary has aimed at, namely the virtual IP address, will soon be out of date.

B. ASD in SD-UWPT

In an SD-UWPT system, ASD is presented to detect power bot attacks on the MPET controller. The basic idea of ASD is as follows.

1) Probing signal $s(t)$ is generated from the information center and sent as an input for the MPET controller.
2) The output of MPET controller $r(t)$ is sent back to the information center and processed by two detection function blocks.
3) The outputs of detection blocks D_1 and D_2 are compared with the look-up table in the information center to determine the type of attack and to locate the attack.

Thus, the attack can be eliminated in a short time. The ASD method is shown in Fig. 4.

1) Active Synchronous Detector Design: The probing signal should have little effect on the normal operation of the MPET controller. One can choose a periodic signal that has little accumulation effect in one period and has a small magnitude, which can be easily filtered out or ignored compared with the reference and feedback signals. Such a probing signal can be

$$s(t) = s(t) + nT \tag{7}$$

$$||s(t)|| < \epsilon \tag{8}$$

$$\int_t^{t+T} s(t)dt = 0. \tag{9}$$

For the detection output, two different detection functions are given as

$$D_1 = \frac{1}{T}\int_t^{t+T} s(t)\cdot r(t)dt \tag{10}$$

$$D_2 = \frac{1}{T}\int_t^{t+T} p\cdot r(t)dt. \tag{11}$$

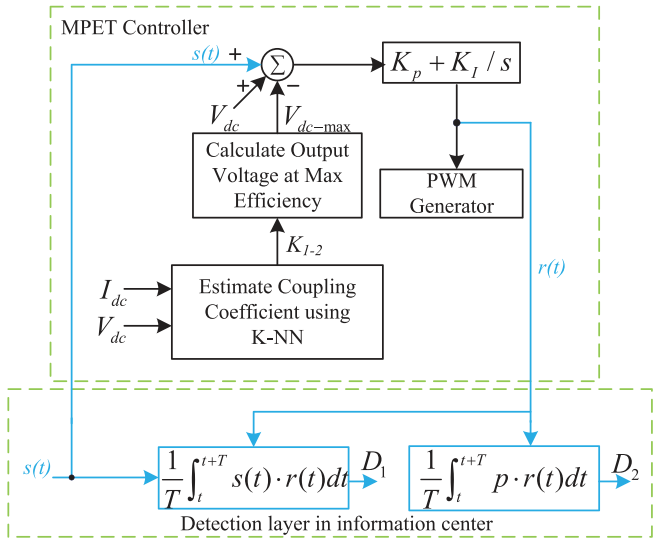


Fig. 4. ASD on MPET controller.

To detect the attack on the MPET, a small sine wave probing signal is generated

$$s(t) = a_0 \sin(w_0 t). \tag{12}$$

The output signal from the PI controller can be derived as

$$r(t) = (V_{\text{dc}} - V_{\text{dc-max}} + s(t)) \cdot (K_P + \frac{K_I}{s}). \tag{13}$$

Therefore, the detection output under normal operations can be expressed as follows:

$$D_1 = \frac{a_0^2 K_p}{2} \tag{14}$$

$$D_2 = p \cdot (V_{\text{dc}} - V_{\text{dc-max}}) \left(K_p + \frac{K_I}{s}\right)$$

$$= p \cdot (r(t) - s(t)) \cdot \left(K_p + \frac{K_I}{s}\right). \tag{15}$$

The details of the deviations are given in Appendix A.

2) Attack Category and Look-Up Table: In this work, following three types of attack against the MPET controller are investigated.

1) Attack I: The parameters of the PI controller K_p are overwritten by the attacker.
2) Attack II: The input to the controller $r(t)$ is modified to a value such that the malicious impact can be induced.
3) Attack III: The k-NN-based machine learning block is attacked such that the maximum reference voltage $V_{\text{dc-max}}$ is modified.

Table I is the look-up table for ASD to detect different attacks.

C. Impedance Measurement Based Approach

The IMBA is proposed to ensure the energy security of the SD-UWPT system. It is comprised of two stages: 1) authorization process and 2) impedance comparison. Here, we briefly derive the equations needed and discuss the two stages later on.

TABLE I
LOOK-UP TABLE FOR ASD

	Normal Operation	Attack I	Attack II	Attack III	Attack I and II	Attack I and III
D_1	$\frac{a_0^2 K_p}{2}$	$\frac{a_0^2 K_p{}'}{2}$	0	$\frac{a_0^2 K_p}{2}$	0	$\frac{a_0^2 K_p{}'}{2}$
D_2	$p \cdot (r(t) - s(t)) \cdot (K_p + \frac{K_I}{s})$	$p \cdot (r(t) - s(t)) \cdot (K_p{}' + \frac{K_I}{s})$	$p \cdot b \cdot (K_p + \frac{K_I}{s})$	$p \cdot (r(t)' - s(t)) \cdot (K_p + \frac{K_I}{s})$	$p \cdot (r(t) - s(t)) \cdot (K_p{}' + \frac{K_I}{s})$	$p \cdot (r(t)' - s(t)) \cdot (K_p + \frac{K_I}{s})$

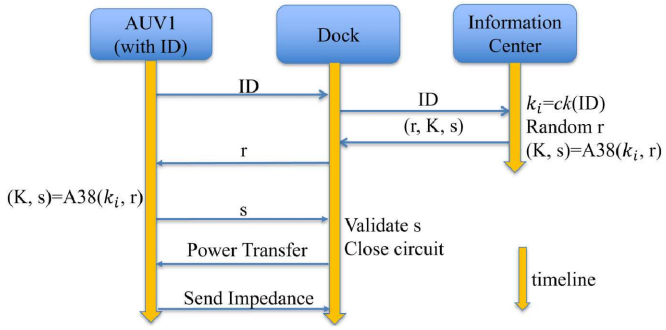


Fig. 5. GSM-based security protocol for SD-UWPT system.

By using KVL in a one-to-one UWPT system, the following equations can be derived:

$$V_1 = jwL_1I_1 - jwL_mI_2 + R_1I_1 + \frac{1}{jwC_1}I_1$$
$$= R_1I_1 - jwL_mI_2 \quad (16)$$
$$0 = jwL_m(I_1 - I_2) - jw(L_2 - L_m)I_2$$
$$- R_2I_2 - Z_LI_2 - \frac{1}{jwC_2}I_2 \quad (17)$$
$$V_2 = I_2Z_L. \quad (18)$$

From these equations, the input impedance from the transmitter side can be expressed as

$$Z_{\text{in}} = \frac{w^2L_m^2}{Z_L + R_2} + R_1 \quad (19)$$

Thus, for one-to-multiple systems, the input impedance can be written as follow:

$$Z_{\text{in}} = R_1 + \sum_{i=2}^{m+1} \frac{(wL_{1i})^2}{Z_{Li} + R_i}. \quad (20)$$

As shown in Fig. 5, for *authorization* of the AUVs, the topology of the global system for mobile communications (GSM) is modeled to enable secure communication. A typical GSM-based security protocol model is built to establish a shared key for the dock and the AUV to securely transfer data. An AUV sends its identification (ID) to a dock, and the dock obtains a random number r, key K, and a validation number s, from the information center. It then sends r to the AUV, if the number s that the AUV sends back is identical to s sent by the information center, then the identity of the AUV is verified. The dock starts to generate power, and asks the authorized AUV to send the input impedance. Existing work has shown the feasibility of applying GSM in the underwater environment. For instance, Fei *et al.* [36] apply GSM short message services to underwater wireless control and transmission systems. Techniques, such as frequency hopping and frequency diversity, are applied to the underwater acoustic communication to mitigate the signal fading and intersymbol interference resulting from the multipath effect. Moreover, in our presented system, acoustic communication can be adopted when the AUVs are far from the docks since optical and electromagnetic waves attenuate fast with the increasing distance in the underwater environment. When AUVs are close to docks, optical and electromagnetic waves are preferred due to their higher speeds. It is shown that the maximum communication distance for the electromagnetic wave can be 6 m when the frequency is 100 kHz [37].

It is worth noting that when authorized AUVs have completed the authorization process and the dock has turned ON the switch, it is likely that an unauthorized AUV steals energy from the dock, as the unauthorized AUV can just get close to the transmitting coil of the dock with no need to verify its identity. In this case, the tasks that are carried out by authorized AUVs will be interrupted. The impedance comparison, the second step of the proposed IMBA, therefore, plays an important role to prevent unauthorized AUVs from stealing energy.

For *impedance comparison*, without a loss of generality, each dock is assumed to maximally charge three AUVs, as shown in Fig. 6. During the charging process, the input impedance on the transmitter side Z_{in} is calculated as the indicator of the number of authorized AUVs. When each authorized AUV plans to receive energy, it sends a message to the dock. Then, the dock sends the verification message and impedance of the AUV to the information center. The information center calculates an estimated value of Z_{in} according to the received impedance and the number of authorized messages, and sends it back to the dock after conducting its calculations. Meanwhile, the dock also measures the actual Z_{in}, and compares the difference between the actual and the estimated values. If the difference is within a certain threshold, then there is no unauthorized AUV. Otherwise, unauthorized AUVs are identified, and the WEC will shut down the charging process. A flowchart of the IMBA is shown in Fig. 7.

IV. TESTING AND VALIDATION OF THE SD-UWPT

In this section, the system shown in Fig. 3 is built to test the performance of the proposed approaches. Specifically, the system consists of an information center, four docks, and multiple AUVs. Each dock is able to charge three AUVs, as shown in Fig. 6. The corresponding network topology is constituted of four switches, four hosts, and one Ryu controller, a widely used SDN controller. The UWPT system is modeled in MATLAB/Simulink under the continuous mode with circuit parameters summarized in Table II. The overall network topology is

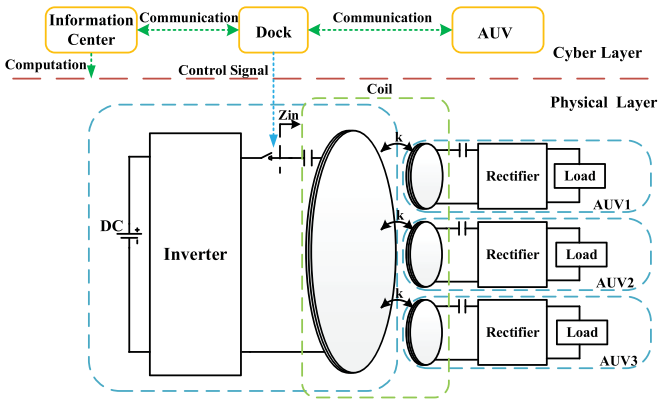


Fig. 6. One-to-multiple UWPT system.

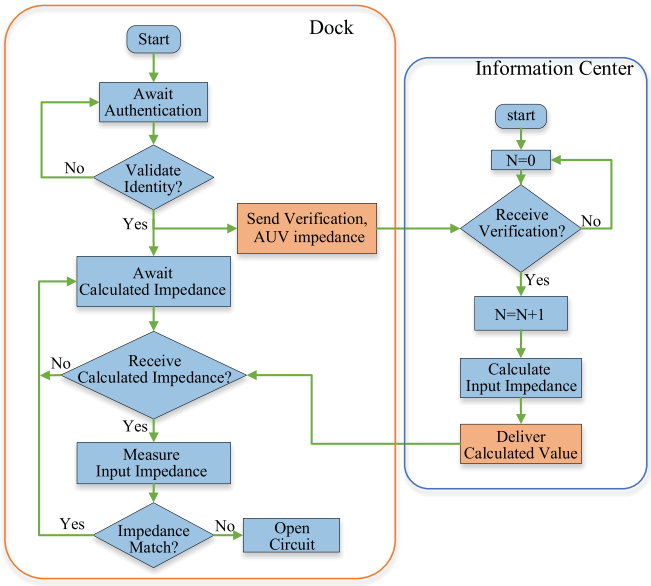


Fig. 7. Flowchart of IMBA.

TABLE II
CIRCUIT PARAMETERS

Parameters	Tx side	Rx side
Self Inductance (μH)	47.8	20.3
Parastic Resistance (Ω)	1.3	1.3
Capacitor (nF)	50	30
Operating Frequency (kHz)	178	178
AC Voltage Source (V)	80	-
Load Resistance (Ω)	-	10, 20, 40

emulated in Mininet [38]. The OpenFlow protocol [39], which enables the remote controlling of the switches' forwarding tables, as aforementioned, is adopted in the SDN topology. User datagram protocol is utilized to transmit data between docks and AUVs through the interface between Simulink and Mininet. Note that the software-defined architecture has shown its feasibility and advantages in practice. For instance, Ren *et al.* [40] establish an SDN-based communication architecture that

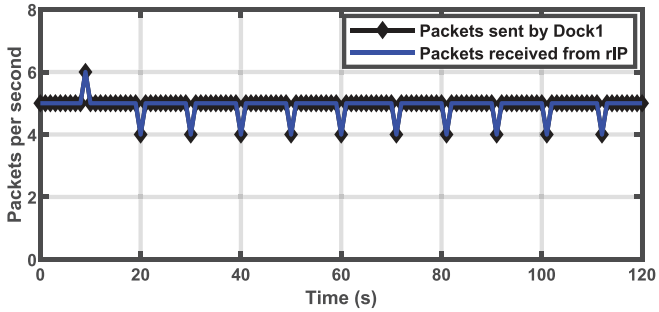


Fig. 8. Data traffic of WEC4.

abstracts the network infrastructure from the upper-level applications to significantly expedite the development of microgrid applications, and create a hardware-in-the-loop cyber-physical platform for evaluating and validating the performance of the presented architecture, control techniques, and SDN-based functionalities. Wang *et al.* [5] develop a software-defined microgrid control scheme, which decouples the control functionality from hardware infrastructure, fully resolving hardware-dependent issues and greatly reduce the cost. Both of the works adopt Mininet to simulate the cyberlayer, and use the real-time simulator, i.e., Opal-RT or RTDS, to simulate the physical layer.

A. *Testing and Validation of the MTD*

The real IP addresses of four hosts, namely four docks, are 10.0.0.1 to 10.0.0.4, respectively. The connections between the docks are tested to validate the effectiveness of the proposed MTD, and two cases are generated.

Case 1. Cyberattacks Without MTD: In this case, data packets are sent from Dock1 to Dock4, whose real IP address is 10.0.0.4. The data traffic received by the real IP address is shown in Fig. 8. It can be seen that the data packets are sent to the real IP address continuously and successfully. Thus, without the MTD, *the real IP address of the docks are exposed to scanners*—The DoS attacks can be easily launched to the hosts since the target is clear and static. The docks under DoS attack will soon be unavailable in the network when the communication links are disabled. Even worse, without the probing signal sent from the docks, further power bot attacks can be launched on the AUVs, causing destructive effects on the whole system.

Case 2. Cyberattacks With MTD: ICMP data packets are generated by Dock1 and sent to Dock4. MTD is enabled in this case, and the virtual IP addresses are assigned to Dock4 with unpredictability. The virtual IPs (vIPs) are randomly chosen from the unused IP address allocations and mutation rate is 0.03 (1 mutation each 30 s). Fig. 9 shows the data traffic sent from Dock1 and received by Dock4. With MTD, the data packets sent to Dock4 are received by the vIPs instead of the real IP. Each vIP is invalid after 30 s. Therefore, Dock4 is unreachable through the real IP address. With MTD, *the real IP addresses of the docks are well protected, whereas the vIPs are out of date very soon.* Thus, the probability that the docks will be vulnerable to a DoS attack is reduced.

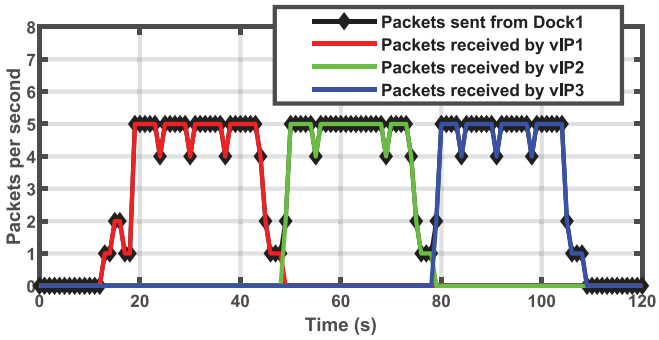


Fig. 9. Data traffic of dock1 and dock4.

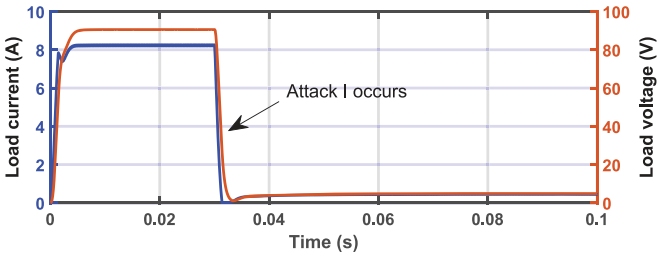


Fig. 10. Load current and voltage under Attack I.

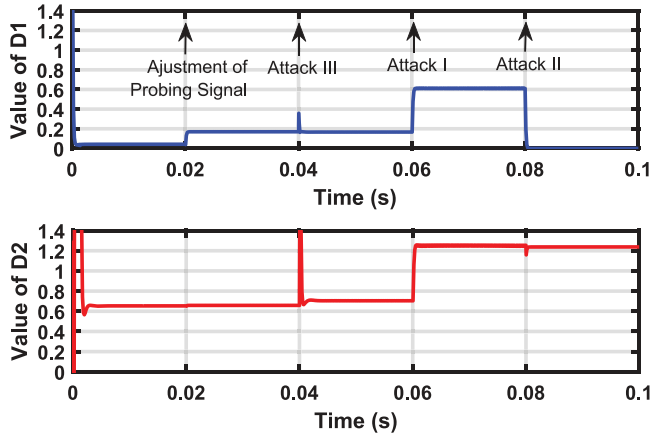


Fig. 11. Detection results of D_1 and D_2.

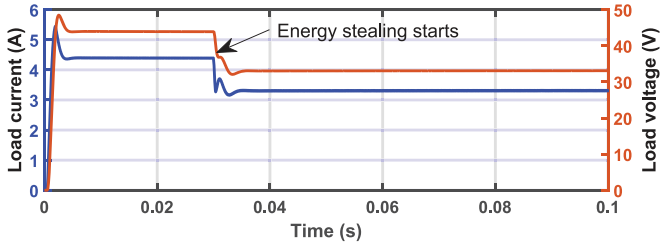


Fig. 12. Load voltage and current of authorized AUV.

B. Testing and Validation of ASD

Based on the MTD, it is reasonable to assume that the communication channels between docks and AUVs are secure. To validate the ASD, two cases are generated. First, performance of the AUVs being charged, namely the load voltage and current are observed without ASD. Second, four tests are launched on the system built in Simulink and Mininet to test the performance of the ASD.

Case 3. Attack I on MPET Without ASD: Attack I is launched on the MPET control at time 0.03 s, where the proportional parameter K_p is modified from 0.28552 to 15. Fig. 10 shows the load voltage and current of the AUV under attack I without ASD. It can be seen that, once the attack is launched, the load voltage and current collapse in a short time. The attacks can easily interrupt the power transfer without ASD. The tasks carried out by the AUV are disrupted because it does not have sufficient residual power.

Case 4. ASD Under Probing Signal Variation and Attacks: Following four tests, including magnitude variations of the probing signal and three other types of attacks, are generated in this case.

1) Magnitude of the probing signal is modified from 0.5 to 1 at time 0.02 s.
2) Attack III is launched at time 0.04 s.
3) Attack I occurs at time 0.06 s, where K_p is modified from 0.28552 to 0.9.
4) Attack II is performed at time 0.08 s.

Fig. 11, which shows the values of $D1$ and $D2$ under four tests, provides corresponding insights, which are as follows.

1) Under probing signal adjustment, $D1$ increases from 0.05 to 0.2, $D2$ remains the same.
2) Under attack III, $D1$ remains unchanged, whereas $D2$ increases from 0.62 to 0.7.
3) Under attack I, $D1$ increases from 0.2 to 0.6 and $D2$ increases from 0.7 to 1.2.
4) Under attack II, $D1$ becomes zero and $D2$ remains unchanged.

The results thus score a 100% detection rate, which verifies the correctness of the detection rules shown in Table I.

From Figs. 10 and 11, it can be seen that, without the ASD, the power bot attacks, which can directly interrupt the power transfer between AUVs and docks, cannot be detected and localized. With ASD, in contrast, *the attacks and the normal adjustment of the probing signal can be precisely detected, which allows further actions to be performed to mitigate the attacks.*

C. Testing and Validation of the IMBA

In this section, three cases, including the observation of load performance without IMBA, as well as the performance of IMBA under different operations and varying loads, are launched to test the performance of the IMBA.

Case 5. Abnormal Operation Without IMBA: In this test, two authorized AUVs are being charged at time 0 s, and a third unauthorized AUV approaches at 0.03 s. The voltage and current responses of the authorized AUV load are shown in Fig. 12. In comparison, Fig. 13 shows the voltage and current responses of the unauthorized AUV load. As can be seen, at time 0.03 s, without IMBA, the load voltage and current of the unauthorized AUV greatly increase, meaning it easily steals energy from the

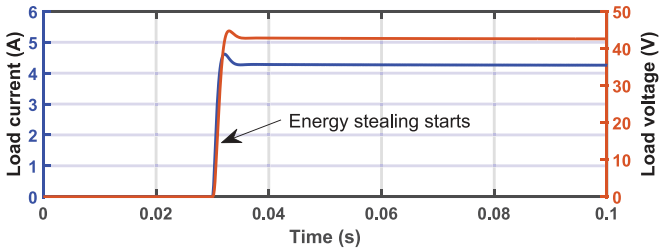
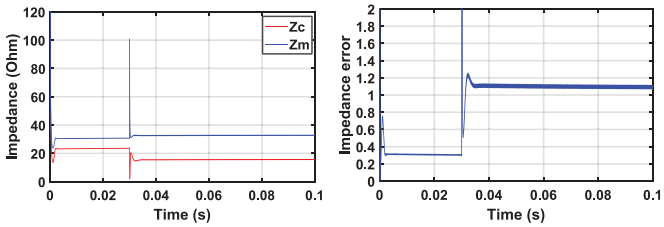


Fig. 13. Load current and voltage of unauthorized AUV.



(a) (b)

Fig. 14. IMBA performance for intrusion detection. (a) Input impedance. (b) Impedance error.

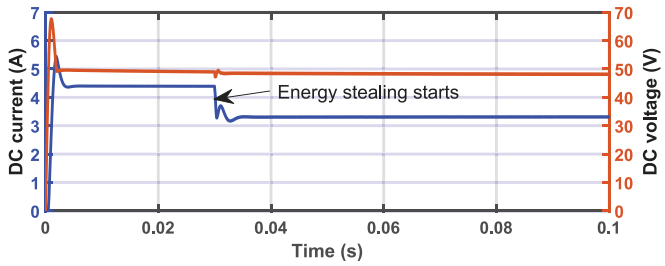
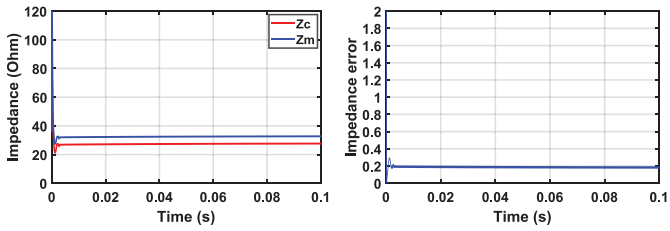


Fig. 15. DC current and voltage.



(a) (b)

Fig. 16. IMBA performance under normal operation: Third authorized AUV being charged from 0 s. (a) Input impedance. (b) Impedance error.

transmitter. Meanwhile, since the whole energy generated by the dock is almost unchanging, the load voltage and load current of the authorized AUV both decrease remarkably, meaning that the power transfer with the dock are greatly weakened by the unauthorized AUV's intrusion.

Case 6: Abnormal Operation With IMBA: In this case, the unauthorized AUV approaches at time 0.03 s. With IMBA, the calculated input impedance and the measured input impedance are obtained by the dock and then compared. As shown in Fig. 14(a), the blue line represents the measured input impedance from the dock side, which is derived by the voltage and current measured from the voltage source in the phasor domain. Meanwhile, the red line represents the calculated input impedance, which equals $R_1 + \sum_{i=2}^{m+1} \frac{w^2 k_{1-2}^2 L_1 L_2}{Z_i}$, where Z_i represents the impedance of the ith authorized AUV. As mentioned earlier, this impedance is sent from the AUV to the dock in the software-defined network. Correspondingly, the impedance error, which equals the difference between the measured and the calculated impedance divided by the measured input impedance, is the key parameter for detecting whether there is an unauthorized AUV intrusion. To detect the unauthorized AUV, the threshold is set constant at 0.3. If the impedance error exceeds 0.3, it indicates that there is an unauthorized AUV stealing energy from the dock. As can be seen from Fig. 14(a), before time 0.03s, the calculated and measured input impedance are very close to each other, and the impedance error is about only 0.2. However, after time 0.03s, the impedance error reaches 1.2. This can be explained in Figs. 14(a) and 15. As the controller works, the dc voltage of the AUV is maintained at the previous level, but the dc current decreases. Thus, impedance Z_i of the authorized AUV increases. Therefore, the calculated impedance on the dock decreases, as shown in Fig. 14(a). For the measured impedance, since there is a third unauthorized AUV also being charged, the actual input impedance equals $R_1 + \frac{w^2 k_{1-2}^2 L_1 L_2}{Z_1} + \frac{w^2 k_{1-2}^2 L_1 L_2}{Z_2} + \frac{w^2 k_{1-2}^2 L_1 L_2}{Z_3}$, where Z_3 is the impedance of the unauthorized AUV. Compared with the previous value, a whole item $\frac{w^2 k_{1-2}^2 L_1 L_2}{Z_3}$ is added to the actual impedance. Therefore, the measured impedance increases greatly after 0.03 s, as shown in Fig. 14(a), the unauthorized AUV intrusion is detected in SDN network.

From Figs. 12 to 15, it shows the following.

1) Without IMBA, the unauthorized AUV can easily steal energy from the dock, because the dock starts to generate power once the authorized ones get their identity verified through the GSM security protocol, and the unauthorized ones can pretend to be authorized ones without verifying their identities.
2) With IMBA, the unauthorized AUVs are detected once they start to get energy from the transmitter. An alarm is raised immediately, and the dock stops the power transfer process immediately.

Case 7. Validation of IMBAs Robustness: To validate the robustness of the IMBA, the performance of IMBA under normal and abnormal operations is observed. Fig. 16 shows the input impedance and corresponding impedance error when the three AUVs are all being charged from time 0, the calculated and measured impedance are in the range between 25 and 30 Ω, and the impedance error is about 0.2 under this situation. Fig. 17 demonstrates the input impedance and impedance error when the third authorized AUV begins charging at time 0.03 s, and the impedance error is around 0.3 and 0.2. Fig. 18 shows that, when the unauthorized AUVs begins charging at time 0, the impedance error becomes 1.2 immediately. These three figures

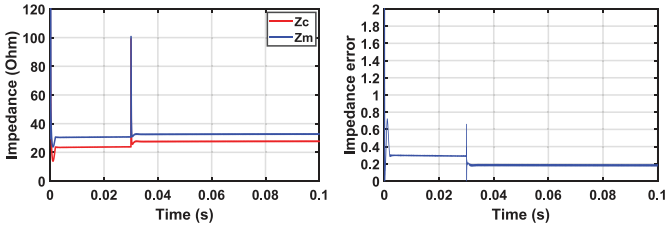


Fig. 17. IMBA performance under abnormal operation: Third authorized AUV being charged from 0.03 s. (a) Input impedance. (b) Impedance error.

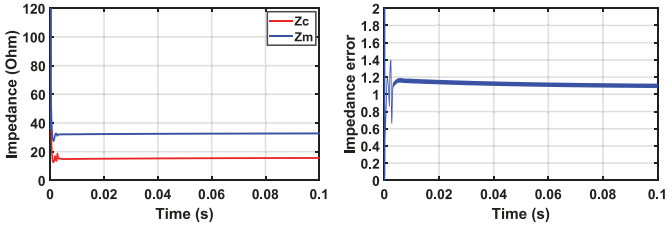


Fig. 18. IMBA performance under abnormal operation: Third authorized AUV being charged from 0 s. (a) Input impedance. (b) Impedance error.

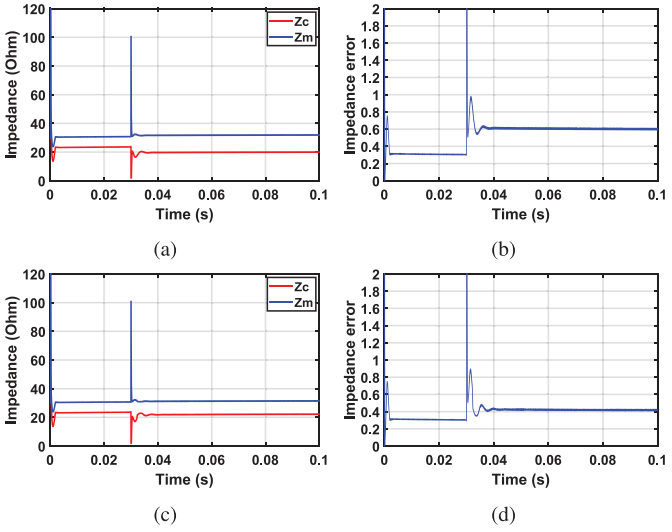


Fig. 19. Input impedance with varying load (a) 20 Ω and (c) 40 Ω and impedance error with varying load (b) 20 Ω and (d) 40 Ω under abnormal operation (the third unauthorized AUV being charged from 0.03 s).

show that, under normal operations, when authorized AUVs are approaching or leaving during the power transfer duration, the impedance error is maintained at a low level, and the alarm would not be triggered in this duration. However, when an unauthorized AUV starts to steal energy, the impedance error increases greatly. Therefore, *the IMBA features a high true positive rate as well as a negative rate*.

In previous tests, the load of the unauthorized AUVs was 10 Ω. To further verify the robustness of the IMBA, different loads (20 Ω, 40 Ω) are applied to the AUVs. Fig. 19 shows the input impedance and the impedance error under different loads when unauthorized AUVs start to get energy from the transmitter. As shown in the figure, the gap between the measured and calculated impedance is becoming smaller; thus, the impedance error is decreasing as the load increases. However, the impedance error is still remarkably larger after time 0.03s. *Thus, it shows that IMBA is able to detect the unauthorized AUVs even the load impedance of the AUVs varies with a large range.* Another important point is as follows: At the time instant 0.03 s, as the unauthorized AUV starts to get charged, its impedance at this instant tends to be very small. Meanwhile, the impedance of the authorized AUVs is fairly large. As can be seen in the input impedance, the measured impedance becomes very large because of the small impedance of the unauthorized AUV, whereas the calculated impedance becomes very small in that the large impedance of the authorized AUVs contributes significantly while the impedance of the unauthorized ones are not counted here. The impedance error at 0.03 s can reach up to 50, differing from the impedance error under normal operations where the value never reach such a high level. To summarize, this spike in impedance error is another proof of a robust intrusion detection.

For the energy stealing problem in UWPT systems, very few existing works have investigated the problem. There was one work that focused on energy security in wireless power transfer systems [41]. In that work, energy was encrypted by chaotically regulating the frequency of the power source. Then, the authorized receptor could receive the energy by simultaneously adjusting the circuit to decrypt the encrypted energy with the security key obtained from the power supply, whereas the unauthorized receptor could not receive the energy with no knowledge of the security key. However, this method has its own problems. The receiving power will drop at every interval when the frequency changes. The frequently changing frequency will largely reduce the power efficiency. Compared with the energy encryption method for wireless power transfer systems, our proposed IMBA has the following advantages: 1) the resonant frequency remains constant at 178 kHz, and thus, there would not be power efficiency drop issues caused by the frequently changing resonant frequency; and 2) two steps, *i.e., the authentication and the impedance comparison,* work together to verify the identity of authorized AUVs and detect the unauthorized ones that are stealing energy from the docks.

V. Conclusion

In this article, a cyber and energy-secure SD-UWPT system was proposed. MTD was found effective in protecting the SD-UWPT from scanning attacks such as DoS attack. Based on the secure communication layer, ASD on MPET was devised to protect the dc–dc converter from power bot attack. IMBA was incorporated to detect the intrusion of unauthorized AUVs, thus ensuring the security of the energy transfer. Extensive tests and case studies are performed to validate the effectiveness of SD-UWPT. Our future work is to develop high-power applications for UWPT.

TABLE III
EQUATION NOTATIONS

R_1, R_2	Parastic resistance of transmitter, receiver coils
L_1, L_2	Self Inductance of transmitter, receiver coils
C_1, C_2	Resonant capacitance of transmitter, receiver
Z_L	Load impedance
V_1, V_2	Voltage of transmitter, receiver coils
I_1, I_2	Current of transmitter, receiver coils
P_1, P_2	Power of transmitter, receiver
η	Power efficiency
K_p, K_s	Proportional, integral coefficient of MPET controller.
w	Resonant frequency (operating frequency) of UWPT system
w_0	Frequency of probing signal

APPENDIX A
DERIVATION OF ASD

According to (10), (12), and (13), we have

$$\begin{aligned} D_1 &= \frac{1}{T}\int_t^{t+T} s(t)\cdot r(t)dt \\ &= \frac{1}{T}\int_t^{t+T} a_0\sin(w_0t)\left(V_{\text{dc}} - V_{\text{dc-max}} + s(t)\right) \\ &\quad \cdot\left(K_P + \frac{K_I}{s}\right)dt \\ &= \frac{1}{T}\int_t^{t+T} a_0\sin(w_0t)V_{\text{dc}}\left(K_P + \frac{K_I}{s}\right)dt \\ &\quad - \frac{1}{T}\int_t^{t+T} a_0\sin(w_0t)V_{\text{dc-max}}\left(K_P + \frac{K_I}{s}\right)dt \\ &\quad + \frac{1}{T}\int_t^{t+T} a_0^2\sin^2(w_0t)\left(K_P + \frac{K_I}{s}\right)dt \end{aligned} \tag{21}$$

where the notations are given in Table III. Since V_{dc} and $V_{\text{dc-max}}$ are constant, the first two items of the previous integration become zero. Thereby

$$\begin{aligned} D_1 &= \frac{1}{T}\int_t^{t+T} a_0^2\sin^2(w_0t)\left(K_P + \frac{K_I}{s}\right)dt \\ &= \frac{a_0^2}{2}\left(K_P + \frac{K_I}{s}\right). \end{aligned} \tag{22}$$

When the frequency of the probing signal is large enough, D_1 ends up with

$$D_1 = \frac{a_0^2}{2}K_P. \tag{23}$$

As for D_2, according to (11) and (13), it can be expressed as follows:

$$\begin{aligned} D_2 &= \frac{1}{T}\int_t^{t+T} p\cdot\left(V_{\text{dc}} - V_{\text{dc-max}} + s(t)\right)\left(K_p + \frac{K_I}{s}\right)dt \\ &= \frac{1}{T}\int_t^{t+T} p\cdot\left(V_{\text{dc}} - V_{\text{dc-max}}\right)\cdot\left(K_p + \frac{K_I}{s}\right)dt \\ &\quad + \frac{1}{T}\int_t^{t+T} p\cdot s(t)dt. \end{aligned} \tag{24}$$

Since the second term of the previous integration is zero, D_2 can be expressed as

$$\begin{aligned} D_2 &= p\cdot\left(V_{\text{dc}} - V_{\text{dc-max}}\right)\left(K_p + \frac{K_I}{s}\right) \\ &= p\cdot\left(r(t) - s(t)\right)\cdot\left(K_p + \frac{K_I}{s}\right). \end{aligned} \tag{25}$$

REFERENCES

[1] T. M. Hayslett, T. Orekan, and P. Zhang, "Underwater wireless power transfer for ocean system applications," in *Proc. OCEANS MTS/IEEE Monterey*, Sep. 2016, pp. 1–6.

[2] C.-C. Kao, Y.-S. Lin, G.-D. Wu, and C.-J. Huang, "A comprehensive study on the Internet of underwater things: Applications, challenges, and channel models," *Sensors*, vol. 17, no. 7, 2017, Art. no. 1477.

[3] T. Kan, R. Mai, P. P. Mercier, and C. C. Mi, "Design and analysis of a three-phase wireless charging system for lightweight autonomous underwater vehicles," *IEEE Trans. Power Electron.*, vol. 33, no. 8, pp. 6622–6632, Aug. 2018.

[4] T. Orekan and P. Zhang, *Underwater Wireless Power Transfer: Smart Ocean Energy Converters*. Berlin, Germany: Springer-Verlag, 2019.

[5] L. Wang, Y. Qin, Z. Tang, and P. Zhang, "Software-defined microgrid control: The genesis of decoupled cyber-physical microgrids," *IEEE Open Access J. Power Energy*, vol. 7, pp. 173–182, June 2020.

[6] I. F. Akyildiz, P. P. Wang, and S.-C. Lin, "SoftWater: Software-defined networking for next-generation underwater communication systems," *Ad Hoc Netw.*, vol. 46, pp. 1–11, 2016.

[7] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in *Proc. IEEE SDN Future Netw. Serv.*, 2013, pp. 1–7.

[8] H. Wang, L. Xu, and G. Gu, "FloodGuard: A DoS attack prevention extension in software-defined networks," in *Proc. 45th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2015, pp. 239–250.

[9] Y. Li, Y. Qin, P. Zhang, and A. Herzberg, "SDN-enabled cyber-physical security in networked microgrids," *IEEE Trans. Sustain. Energy*, vol. 10, no. 3, pp. 1613–1622, Jul. 2019.

[10] M. Canini, D. Venzano, P. Perešíni, D. Kostić, and J. Rexford, "A NICE way to test OpenFlow applications," in *Proc. NSDI*, 2012, pp. 127–140.

[11] E. Al-Shaer and S. Al-Haj, "FlowChecker: Configuration analysis and verification of federated OpenFlow infrastructures," in *Proc. 3rd ACM Workshop Assurable Usable Secur. Configuration*, 2010, pp. 37–44.

[12] T. Hinrichs, N. Gude, M. Casado, J. Mitchell, and S. Shenker, "Expressing and enforcing flow-based network security policies," University of Chicago, Tech. Rep., vol. 9, 2008.

[13] S. Misra, S. Dash, M. Khatua, A. V. Vasilakos, and M. S. Obaidat, "Jamming in underwater sensor networks: Detection and mitigation," *IET Commun.*, vol. 6, no. 14, pp. 2178–2188, 2012.

[14] Q. Wang, H.-N. Dai, X. Li, and H. Wang, "Eavesdropping attacks in underwater acoustic networks," in *Proc. 10th Int. Conf. Inf. Commun. Signal Process.*, 2015, pp. 1–5.

[15] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 1, pp. 729–752, Jan.–Mar. 2018.

[16] L. Xiao, Q. Li, T. Chen, E. Cheng, and H. Dai, "Jamming games in underwater sensor networks with reinforcement learning," in *Proc. IEEE Global Commun. Conf.*, 2015, pp. 1–6.

[17] X. Li, G. Han, A. Qian, L. Shu, and J. Rodrigues, "Detecting Sybil attack based on state information in underwater wireless sensor networks," in *Proc. 21st Int. Conf. Softw. Telecommun. Comput. Netw.*, 2013, pp. 1–5.

[18] C. Wang and Z. Wang, "Signal alignment for secure underwater coordinated multipoint transmissions," *IEEE Trans. Signal Process.*, vol. 64, no. 23, pp. 6360–6374, Dec. 2016.

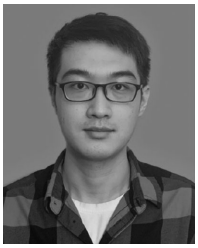
[19] S. Basagni, C. Petrioli, R. Petroccia, and D. Spaccini, "CARP: A channel-aware routing protocol for underwater acoustic wireless networks," *Ad Hoc Netw.*, vol. 34, pp. 92–104, 2015.

[20] Y. Huang, S. Zhou, Z. Shi, and L. Lai, "Experimental study of secret key generation in underwater acoustic channels," in *Proc. 48th Asilomar Conf. Signals Syst. Comput.*, 2014, pp. 323–327.

[21] H. Yan, Z. J. Shi, and Y. Fei, "Efficient implementation of elliptic curve cryptography on DSP for underwater sensor networks," in *Proc. 7th Workshop Optim. DSP Embedded Syst.*, 2009, pp. 7–15.

[22] J. E. Faugstadmo, M. Pettersen, J. M. Hovem, A. Lie, and T. A. Reinen, "Underwater wireless sensor network," in *Proc. 4th Int. Conf. Sens. Technol. Appl.*, 2010, pp. 422–427.

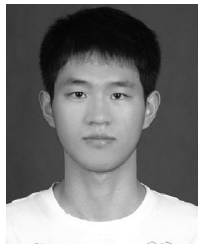
[23] M.-F. Hsieh, I.-H. Lin, D. G. Dorrell, M.-J. Hsieh, and C.-C. Lin, "Development of a wave energy converter using a two chamber oscillating water column," *IEEE Trans. Sustain. Energy*, vol. 3, no. 3, pp. 482–497, Jul. 2012.
[24] D. I. Forehand, A. E. Kiprakis, A. J. Nambiar, and A. R. Wallace, "A fully coupled wave-to-wire model of an array of wave energy converters," *IEEE Trans. Sustain. Energy*, vol. 7, no. 1, pp. 118–128, Jan. 2016.
[25] H. Kaushal and G. Kaddoum, "Underwater optical wireless communication," *IEEE Access*, vol. 4, pp. 1518–1547, Apr. 2016.
[26] M. Ayaz and A. Abdullah, "Hop-by-hop dynamic addressing based (H2-DAB) routing protocol for underwater wireless sensor networks," in *Proc. Int. Conf. Inf. Multimedia Technol.*, 2009, pp. 436–441.
[27] N. Javaid *et al.*, "An efficient data-gathering routing protocol for underwater wireless sensor networks," *Sensors*, vol. 15, no. 11, pp. 29149–29181, 2015.
[28] H. Wu, X. Chen, C. Shi, Y. Xiao, and M. Xu, "An ACOA-AFSA fusion routing algorithm for underwater wireless sensor network," *Int. J. Distrib. Sens. Netw.*, vol. 8, no. 5, 2012, Art. no. 920505.
[29] J.-H. Cui, J. Kong, M. Gerla, and S. Zhou, "The challenges of building scalable mobile underwater wireless sensor networks for aquatic applications," *IEEE Netw.*, vol. 20, no. 3, pp. 12–18, May/Jun. 2006.
[30] J. Heidemann, W. Ye, J. Wills, A. Syed, and Y. Li, "Research challenges and applications for underwater sensor networking," in *Proc. IEEE Wireless Commun. Netw. Conf.*, 2006, pp. 228–235.
[31] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22–28, Mar. 2011.
[32] B. Drew, A. R. Plummer, and M. N. Sahinkaya, "A review of wave energy converter technology," *Proc. Inst. Mech. Eng., Part A*, vol. 223, pp. 887–902, 2009.
[33] T. Orekan, P. Zhang, and C. Shih, "Analysis, design, and maximum power-efficiency tracking for undersea wireless power transfer," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 6, no. 2, pp. 843–854, Jun. 2018.
[34] Y. Cong, G. Yang, Z. Wei, and W. Zhou, "Security in underwater sensor network," in *Proc. IEEE Int. Conf. Commun. Mobile Comput.*, 2010, vol. 1, pp. 162–168.
[35] J. H. Jafarian, E. Al-Shaer, and Q. Duan, "OpenFlow random host mutation: Transparent moving target defense using software defined networking," in *Proc. 1st Workshop Hot Topics Softw. Defined Netw.*, 2012, pp. 127–132.
[36] Y. Fei, C. En, and H. LianFen, "Underwater wireless control and transmission system based on GSM short message," in *Proc. IEEE Int. Conf. Commun. Circuits, Syst.*, 2006, vol. 4, pp. 2515–2519.
[37] J. Lloret, S. Sendra, M. Ardid, and J. J. Rodrigues, "Underwater wireless sensor communications in the 2.4 GHz ISM frequency band," *Sensors*, vol. 12, no. 4, pp. 4237–4264, 2012.
[38] "Mininet." Accessed: Aug. 1, 2019. [Online]. Available: http://mininet.org
[39] N. McKeown *et al.*, "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 38, no. 2, pp. 69–74, 2008.
[40] L. Ren, Y. Qin, B. Wang, P. Zhang, P. B. Luh, and R. Jin, "Enabling resilient microgrid through programmable network," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2826–2836, Nov. 2017.
[41] Z. Zhang, K. Chau, C. Qiu, and C. Liu, "Energy encryption for wireless power transfer," *IEEE Trans. Power Electron.*, vol. 30, no. 9, pp. 5237–5246, Sep. 2015.



Jiangwei Wang (Student Member, IEEE) received the B.S. degree in electrical and computer engineering from Xi'an Jiaotong University, Xi'an, China, in 2018. He is currently working toward the Ph.D. degree with the Electrical and Computer Engineering Department, University of Connecticut, Storrs, CT, USA.

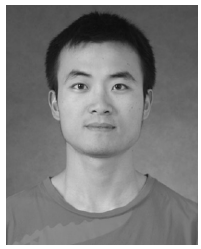
His current research interests include cyber–physical systems.

Mr. Wang was a recipient of Outstanding Reviewer for the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY and IEEE JOURNAL OF OCEANIC ENGINEERING in 2019.



Yanyuan Qin (Student Member, IEEE) received the B.S. degree in automation from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2011, and the M.S. degree in control science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2014. He is currently working toward the Ph.D. degree with the Computer Science and Engineering Department, University of Connecticut, Storrs, CT, USA.

His research interests include software-defined networking and wireless networks.



Zefan Tang (Student Member, IEEE) received the B.S. degree in mechanical engineering from Zhejiang University, Zhejiang, China, in 2014, and the M.S. degree in electrical and computer engineering from the University of Michigan-Shanghai Jiao Tong University Joint Institute, Shanghai Jiao Tong University, Shanghai, China, in 2017. He is currently working toward the Ph.D. degree in electrical engineering with Stony Brook University, Stony Brook, NY, USA.

His current research interests include microgrids, quantum security, quantum key distribution, quantum networking, and cyber-physical security for electric power networks.

Mr. Tang is a recipient of the Best Presentation Recognition in 2015 Annual Conference of the IEEE Industrial Electronics Society and the Best Paper Award in 2020 IEEE Power & Energy Society General Meeting. He was also a recipient of the Outstanding Reviewer for the IEEE TRANSACTIONS ON POWER SYSTEMS in 2018.

Peng Zhang (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of British Columbia, Vancouver, BC, Canada, in 2009.

He is currently a SUNY Empire Innovation Professor with Stony Brook University, New York, Stony Brook, NY, USA. He is an affiliated Staff Scientist with Brookhaven National Laboratory and an affiliated Professor of Computer Science and Applied Mathematics and Statistics with Stony Brook University. Previously, he was a Centennial Associate Professor and a Francis L. Castleman Associate Professor with the University of Connecticut, Storrs, CT, USA. He was a System Planning Engineer with BC Hydro and Power Authority, Vancouver, BC, Canada, during 2006–2010. His research interests include programmable microgrids, networked microgrids, quantum-engineered resilient grids, quantum computing, AI-driven smart grid, quantum security, power system reachability, and quantum networking.

Dr. Zhang is an individual member of CIGRÉ. He is an Editor for the IEEE TRANSACTIONS ON POWER SYSTEMS, the IEEE TRANSACTIONS ON SUSTAINABLE ENERGY, and the IEEE POWER AND ENERGY SOCIETY LETTERS, and an Associate Editor for the IEEE JOURNAL OF OCEANIC ENGINEERING.