On the Vulnerability of Underwater Magnetic Induction Communication

Muhammad Muzzammil, Waqas Aman, Irfan Ullah, Shang Zhigang, Saif Al-Kuwari, *Senior Member, IEEE*, Zhou Tian, Marwa Qaraqe, *Senior Member, IEEE*

***Abstract*—Typical magnetic induction (MI) communication is commonly considered a secure underwater wireless communication (UWC) technology due to its non-audible and non-visible nature compared to acoustic and optical UWC technologies. However, vulnerabilities in communication systems inevitably exist and may lead to different types of attacks. In this paper, we investigate the eavesdropping attack in underwater MI communication to quantitatively measure the system's vulnerability under this attack. We consider different potential eavesdropping configuration setups based on the positions and orientations of the eavesdropper node to investigate how they impact the received voltage and secrecy at the legitimate receiver node. To this end, we develop finite-element-method-based simulation models for each configuration in an underwater environment and evaluate the received voltage and the secrecy capacity against different system parameters such as magnetic flux, magnetic flux density, distance, and orientation sensitivity. Furthermore, we construct an experimental setup within a laboratory environment to replicate the simulation experiments. Both simulation and lab experimental confirm the susceptibility of underwater MI communication to eavesdropping attacks. However, this vulnerability is highly dependent on the position and orientation of the coil between the eavesdropper and the legitimate transmitter. On the positive side, we also observe a unique behavior in the received coil reception that might be used to detect malicious node activities in the vicinity, which might lead to a potential security mechanism against eavesdropping attacks.**

***Index Terms*—Magnetic induction, eavesdropping, vulnerability, underwater, distance, orientation sensitivity, secrecy capacity, received power, and finite element method.**

I. Introduction

Underwater wireless communication (UWC) technologies such as acoustic, optics, electromagnetic, and magnetic induction (MI) facilitate the exploration of vast oceanic systems, which are rich in plentiful natural resources such as oil and gas, and play a significant role in essential applications, such as combating climate change and underwater monitoring [1], [2]. In addition, UWC technologies are also widely used in military and surveillance applications [3], [4]. The choice of UWC technologies should be application-dependent, as the harsh nature of the underwater environment greatly affects communication channels, which have unique characteristics according to the underlying technology [5], [6].

Acoustic communication is widely used in underwater environments due to the long propagation nature of acoustic waves, making it the most feasible option for long-distance communication. However, it faces significant challenges such as low data rate, high link delay, large multipath, and the Doppler effect [2], [7]. On the other hand, underwater optical wireless communication can be ideal for high data rates, low link delay, and medium-range communication, but it experiences high attenuation, scattering, and line of sight requirements [8]. Magnetic induction (MI) communication has recently emerged as a promising alternative for medium-range underwater applications, offering stable channel response, absence of multipath and Doppler effects, and smooth cross-boundary communication due to the same magnetic permeability in air and water [2], [9]. However, MI communication faces challenges related to the orientation of the coil and the conductive nature of water [10].

UWC technologies suffer from intrinsic vulnerabilities due to their broadcast nature. This makes UWC (like other wireless technologies) susceptible to conventional wireless communication attacks, including eavesdropping [11] and jamming [6]. In the literature, numerous studies have investigated the vulnerabilities of underwater acoustic communication [6], [12]–[14]. Similarly, vulnerabilities in underwater optical communication have also been reported [15]–[17]. However, studies on the vulnerabilities of underwater magnetic induction communication are quite rare and are mainly focused on short-range near-field communication (NFC) [18]–[23].

In [18], the authors summarize various security attacks on NFC communication. A similar study is reported in [19], which provides a classification of near-field communication attacks and discusses security concerns in NFC by targeting mainly five short-range applications such as healthcare and e-payment. [22] presented the vulnerabilities in NFC and focused on the denial of service attack and data corruption attack. In [23], the authors studied broken access control attacks, especially in e-payment services that use NFC technology. Security in wireless power transfer applications based on magnetic coupling is studied in [20], and countermeasure techniques for eavesdropping in NFC are studied in [21]. In [24], the authors studied the secrecy capacity of a simultaneous

This work is partially funded by the G5828 "SeaSec: DroNets for Maritime Border and Port Security" project under the NATO's Science for Peace Programme.

Muhammad Muzzammil, Irfan Ullah, Shang Zhigang, and Zhou Tian are with the Acoustic Science and Technology Laboratory, Harbin Engineering University, Harbin 150001, China, the Key Laboratory of Marine Information Acquisition and Security, Harbin Engineering University, Ministry of Industry and Information Technology, Harbin 150001, China, and the College of Underwater Acoustic Engineering, Harbin Engineering University, China, Email: {muzzammilm, irfankhan, shangzhigang, zhoutian}@hrbeu.edu.cn.

W. Aman, S. Al-Kuwari and M. Qaraqe are with the Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar, Emails: {waman, smalkuwari, mqaraqe}@hbku.edu.qa.

Corresponding Author: Muhammad Muzzammil, Email: muzzammilm@hrbeu.edu.cn

wireless information and power transfer system based on magnetic inductive coupling. Since these studies are based on NFC with a range of up to $\approx 10cm$, their target applications are mainly healthcare, e-payment, and tracking. However, in this paper, we quantitatively study the vulnerabilities of MI-based underwater wireless communication against eavesdropping attacks and show that MI is indeed susceptible to such attacks. The main contributions made in this paper are summarized in following subsection.

A. Contribution

In this paper, we investigate the eavesdropping attack on underwater MI communication. In a typical eavesdropping scenario, the eavesdropper node can receive a magnetic field and, when approaching the vicinity of legitimate ongoing MI communication, can listen to the legitimate communication (see Section II-B). Hence, we consider an underwater environment with three nodes: one legitimate transmitter (Tx) node, one legitimate receiver (Rx) node, and one eavesdropper node. The contributions of this paper can be summarized as follows:

- We analyze a system model for an eavesdropping attack on legitimate underwater MI communication by considering two main challenges: the placement and orientation sensitivity of the eavesdropper node with respect to the legitimate nodes. We attempt to address two main questions: *First*, whether and how much information an eavesdropper node can receive from an ongoing legitimate MI communication. *Second*, whether legitimate nodes can detect malicious activity in the environment.
- We develop various configurations to assess the impact of the position and orientation of the eavesdropper node on legitimate nodes. In the position case, we use two different configurations based on the far and near position of an eavesdropper node with respect to legitimate nodes. In the orientation case, we use three different configurations; changing the orientation of an eavesdropper node in a rotational fashion with respect to legitimate Tx, Rx, and around its own origin. We develop a finite element method (FEM) simulation for underwater MI communication models (based on various configurations mentioned earlier) to quantitatively measure the vulnerability (Section III).
- To verify the FEM simulation results, we further conduct lab experiments (Section III-C).

B. Organization

The rest of this paper is organized as follows: Section II provides a brief background on MI communication and eavesdropping attack. The evaluation of our system model using FEM simulation is presented in Section III followed by experimental validation in Section III-C. Finally, the paper concludes in Section IV with a few concluding remarks and future directions.

II. Preliminaries

A. MI Communication

MI communication works as follows: a pair of low-cost wounded coils are used, where one coil (Tx) is excited with a time-varying signal to generate a time-varying magnetic field B, given by [25], [26]

$$B = \frac{\mu_0 I_{Tx} N r^2 cos(\theta)}{2(r^2 + d^2)^{3/2}}, \tag{1}$$

where $\mu_0 = 4\pi \times 10^{-7}$ is the permeability constant, N is the number of turns, I_{Tx} is the time-varying current supplied to the Tx coil, r is the radius of the coil, d is the distance from the Tx coil, and θ is the angle between the Tx and Rx coils. Eq. (1) can be used in air medium that is a non-conducting medium, however, the magnetic field signals can be further attenuated due to eddy current in a conducting medium such as seawater. The magnetic field therefore becomes [26]

$$B = \frac{\mu_0 N_{\mathrm{w}} I_{Tx} r^2 \cos(\theta)}{2(r^2 + d^2)^{3/2}} \, e^{-\frac{\sqrt{d^2+r^2}}{\delta}}, \tag{2}$$

where $\delta = \frac{1}{\sqrt{\pi f \mu \sigma}}$ represents the skin depth (in the case of good conductors) and σ is the conductivity of the medium. The receiver coil couples with the Tx coil when it comes closer to it and voltage is induced (V_{ind}) to the Rx coil, which can be expressed as [25], [27]

$$V_{ind} = 2\pi N A B cos(\theta), \tag{3}$$

where N and A denote the number of turns and area of the coil, B is the magnetic field strength, and θ is the angle of arrival. Therefore, the two coils coupled with each other, and this coupling is equal to $k = M/\sqrt{L_{Tx} L_{Rx}}$ [28], where L_{Tx} and L_{Rx} denote the inductance values of Tx and Rx coils, while M is the mutual inductance between the two coils and can be expressed as [2], [29]

$$M = \frac{\mu_r \mu_0 \pi N_{Tx} r_{Tx}^2 N_{Rx} r_{Rx}^2}{2\sqrt{\left(r_{Tx}^2 + d^2\right)^3}}, \tag{4}$$

where $\mu_o = 4\pi \times 10^7 H/m$ is the magnetic permeability constant and $\mu_r = 1$ is the relative permeability of water; N_{Tx} and N_{Rx} are the number of turns of the Tx and Rx coil, r_{Tx} and r_{Rx} is the radius of the Tx and Rx coil and d is the distance between Tx and Rx coil.

The coupling strength of the Tx-Rx coils can be described in many terms, such as the value of the coupling coefficient (range between 0 and 1) or the received voltage at the receiver. A coupling coefficient with a value 1 means that Tx and Rx are strongly coupled, while a value 0 means that they are no longer coupled. Similarly, the maximum voltage received at the Rx coil means strong coupling and vice versa. Furthermore, strong coupling depends on many factors, such as how close the coils are to each other and the magnetic moment, which is $m = NIAcos(\theta)$, where N, A, and I denote the number of turns, the area of the coil, and the current supplied to the Tx coil. θ represents the angle between the Tx and Rx coil.

The communication range through MI directly depends on the magnetic moment; increasing magnetic leads to higher received magnetic field strength, which facilitates longer communication distance and vice versa. Since the attenuation rate of the magnetic field strength decays very rapidly ($1/d^3$, where

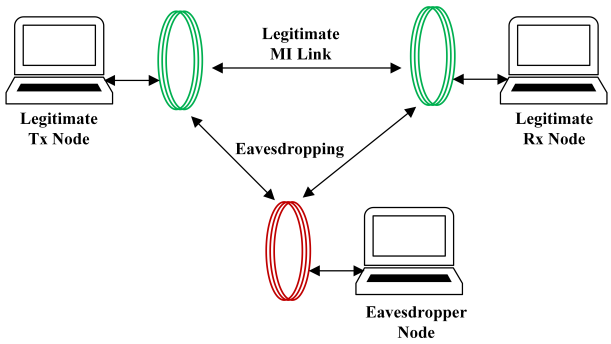


Fig. 1: General illustration of an eavesdropping attack.

d is the communication distance), one of the major challenges in MI communication is the limited range.

The angle term in the magnetic moment introduces an important challenge in MI communication; that is, when $\theta = 0°$, Tx and Rx coils are perfectly aligned, meaning that Rx receives the maximum magnetic field strength. On the other hand, if $\theta \neq 0°$, Tx and Rx coils are not aligned and Rx consequently receives a weak magnetic field. Therefore, the coil's orientation between any two MI communicating nodes plays a significant role in MI communication. In the following sections, we focus on these main challenges of MI communication in our study of eavesdropping attacks.

B. Eavesdropping

An eavesdropping attack, also known as passive wiretapping or snooping, is a form of unauthorized interception of communications between two parties. This attack involves an adversary secretly monitoring and listening to conversations, data transmissions, or any form of communication between intended participants without their knowledge or consent. An eavesdropping attack is therefore considered a breach of privacy and security and can have serious consequences, such as compromise of critical infrastructure, identity, and data theft.

We consider MI communication between two legitimate nodes: Tx and Rx under the water with the presence of an eavesdropper node in closed proximity that aims to listen to the ongoing communication as shown in Fig. 1. Since a time-varying sinusoidal signal is applied to the legitimate Tx node on the transmitter side, the legitimate Rx node and the eavesdropper node, therefore, receive the transmitted signal at the receiver side by coming into the vicinity of the generated magnetic field. Various configurations are used to evaluate the eavesdropping attack based on the eavesdropper node position and orientations (detail in Section III).

III. Vulnerability Analysis against Eavesdropping Attacks

We first provide the details of the performance metrics used to investigate the vulnerability of underwater MI communication against eavesdropping attacks. Next, we present two types of quantitative vulnerability studies: one based on FEM simulations and the other based on real-world experiments. It is important to note that, due to the lack of a controlled setup for underwater MI communication experimentation, real-world experiments are conducted in an air medium. This approach is generally accepted, as MI communication is known to perform in a similar fashion across different environments [1], [2], [29], [30]. However, slight variations in the quantitative values may still be observed due to differences in the conductivity of the mediums. These differences arise not only from the disparity in medium conductivity but also from minor mismatches in replicating the simulation model precisely in the real-world experimental setup. Such mismatches can result from uncertainties in hardware devices, including variations in component values such as capacitance and coil inductance, which may introduce additional deviations.

A. Performance Metrics

We used two performance metrics: induced voltage and secret capacity to investigate the system's vulnerability against eavesdropping attacks. Below, we discuss each of them in detail.

1) Induced Voltage: When a signal is transmitted by magnetic induction, it induces a voltage in the receiving coil or conductor. The amplitude of this induced voltage is directly proportional to the strength of the magnetic field and the rate at which it is changing. Therefore, measuring the voltage in the receiver provides information on the strength of the signal that has been successfully transmitted. Additionally, the received power at the receiver coil is a function of the received voltage, as given in Eq. 5. Typically, the induced voltage can be expressed as given in Eq. 3

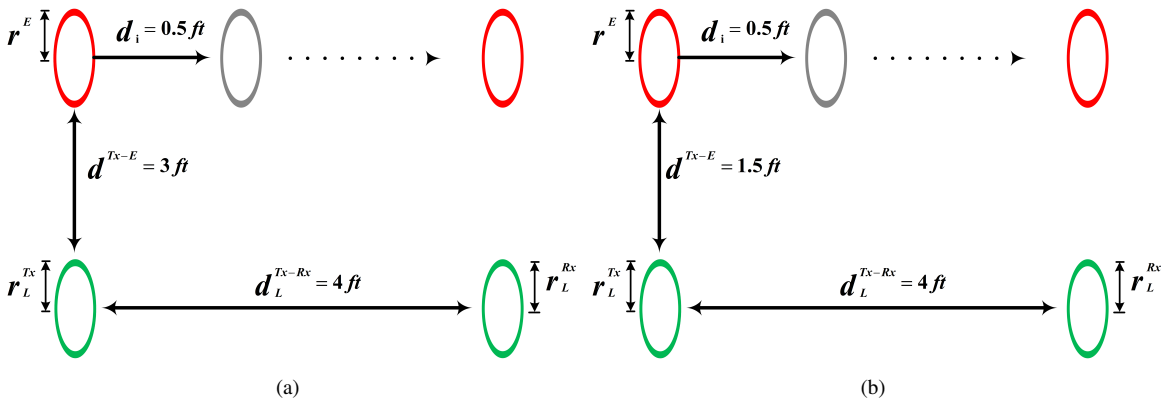
2) Secrecy Capacity: We consider secrecy capacity as a metric for this scenario where the secrecy capacity expression is given as:

$$\text{SC} = \log_2(1 + \text{SNR}_{\text{Rx}}) - \log_2(1 + \text{SNR}_{\text{E}}), \tag{5}$$

where $\text{SNR}_{\text{Rx}} = (\frac{V_{\text{Rx}}^2}{R})/\sigma^2$ and $\text{SNR}_E = (\frac{V_E^2}{R})/\sigma^2$ are the received signal-to-noise ratio of legitimate Rx node and eavesdropper node respectively with $(\frac{V_{\text{Rx}}^2}{R})/(\frac{V_E^2}{R})$ the received power at the legitimate Rx/eavesdropper nodes, $\frac{V_{Rx}}{V_E}$ are the received voltages at legitimate Rx/eavesdropper, R is the load resistance and σ^2 is the noise power.

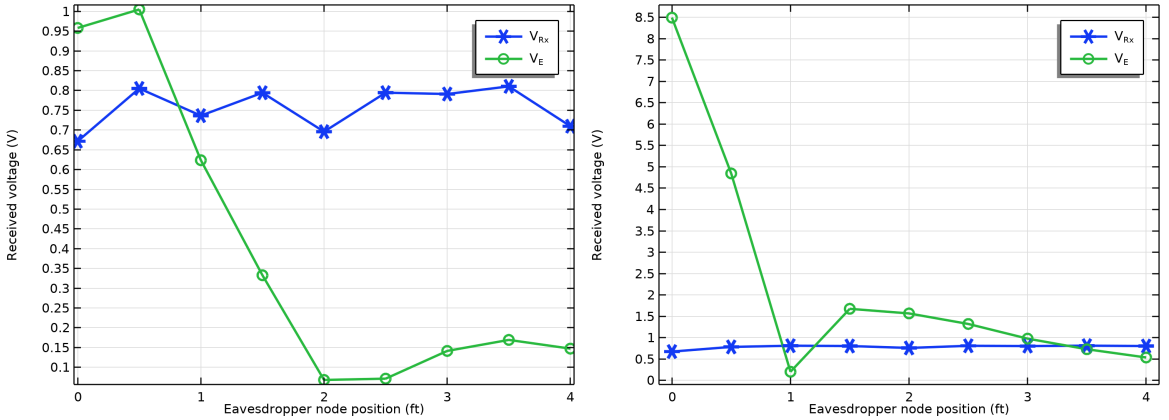
B. FEM-based Simulation

In our simulation experiments, we use FEM simulation to develop the MI communication security model discussed in Section II-B. A sinusoidal voltage signal of $10V$ is applied to Tx. The radius of the coil and the number of turns in the legitimate Tx, legitimate Rx, and eavesdropper nodes remain the same, which is $12.7cm$ and 30, respectively. The capacitor is attached in series with the Tx coil but parallel to the legitimate Rx node and the eavesdropper node to resonate at about $100kHz$ frequency. The capacitance values of the capacitor and coil inductance are listed in Table I. Finally, the conductivity of water is fixed to $0.01S/m$. The parameter values utilized in this study are provided in Table. I, which are the same in overall simulations unless explicitly mentioned.



(a) (b)

Fig. 2: Eavesdropper node position-based setup for both FEM simulation and lab experiments: (**a**) Configuration 1: When the eavesdropper node is placed far from the legitimate nodes and (**b**) Configuration 2: When the eavesdropper node is placed near to the legitimate nodes.



(a) (b)

Fig. 3: Simulation results based on eavesdropper node position with respect to legitimate Tx and Rx positions: (**a**) Received voltage vs. eavesdropper node position under Configuration 1 and (**b**) Received voltage vs. eavesdropper node position under configuration 2.

TABLE I: Parameter settings used in simulations setup.

	Tx node	Rx node	Eavesdropper node
Coil radius	12.7 cm	12.7 cm	12.7 cm
Number of turns	30	30	30
Capacitance	7.681 nF	7.681nF	7.681nF
Inductance	329.75 μH	329.75 μH	329.75 μH
Voltage applied	10 V	-	-
Resonance frequency	100 KHz	100 KHz	100 KHz
Load Resister	-	50 Ω	50 Ω

In the following section, we evaluate the eavesdropping attack based on the position of the eavesdropper node, the orientation of the eavesdropper node, and the secrecy capacity.

1) Eavesdropper node position: In this section, the eavesdropping attack is studied based on the position/placement of the eavesdropper node with respect to legitimate nodes. The position of an eavesdropper node is crucial, as the closer the eavesdropper node is to the legitimate transmitted magnetic field, the more information can be eavesdropped. To study the impact of the position of the eavesdropper node, we consider two different configurations based on how far the eavsdropper node from the legitimate Tx and Rx nodes as shown in Fig. 2. FEM simulation models are developed for two different configurations as depicted in Fig. 2. The detail of the two configurations are below:

1) *Configuration 1:* In this configuration, the eavesdropper is placed far from the legitimate nodes. Initially, the legitimate Tx and Rx nodes are fixed at points (0,0,0)ft and (4,0,0)ft (i.e., $d_L^{Tx-Rx} = 4ft$), respectively. While, the eavesdropper node is initially placed at (0,3,0)ft from the Tx node (i.e., $d^{Tx-E} = 3ft$), and then moves away at an interval of 0.5ft till (4,3,0)ft as depicted in Fig. 2(a).

2) *Configuration 2:* In this configuration, the eavesdropper node is placed closer to the legitimate Tx and Rx nodes. The transmitter node is kept fixed at a point of (0,0,0)ft while a legitimate Rx node is fixed at (4,0,0)ft (i.e., $d_L^{Tx-Rx} = 4ft$). The eavesdropper node is initially placed at (0,1.5,0)ft from the Tx node (i.e.,

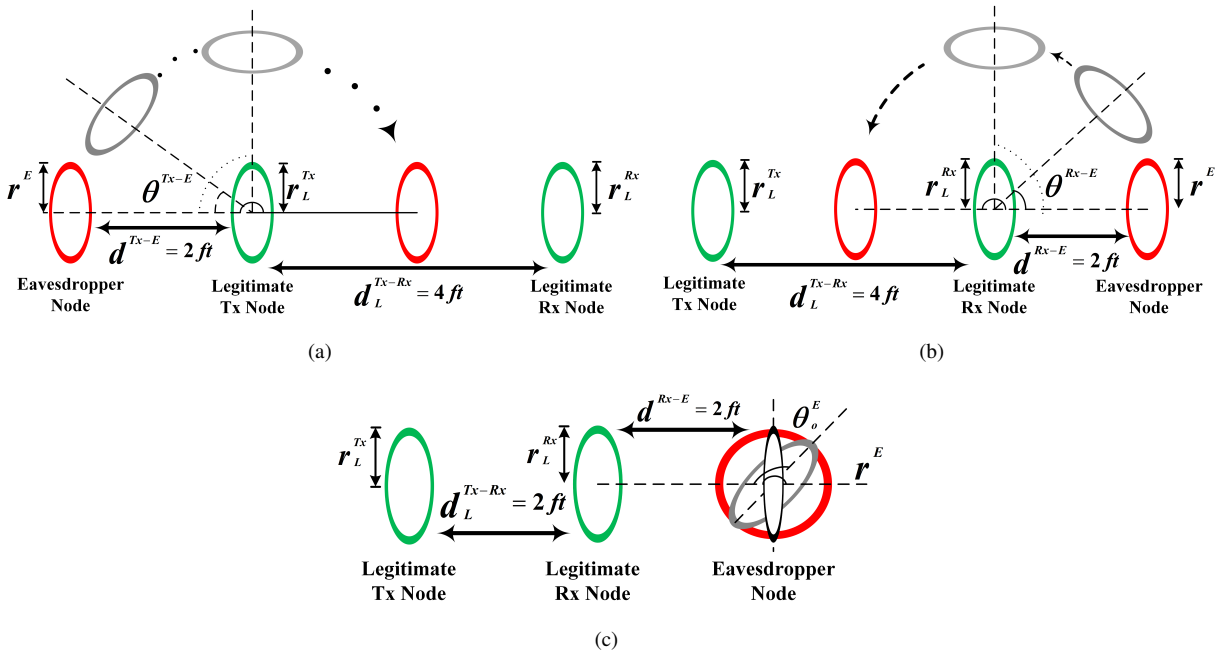


Fig. 4: Eavesdropper node orientation changes (**a**) Configuration 3: eavesdropper changes its position w.r.t. legitimate Tx node, (**b**) Configuration 4: eavesdropper changes its position w.r.t. legitimate Rx node, and (**c**) Configuration 5: eavesdropper changes its position w.r.t. its own origin.

$d^{Tx-E} = 1.5ft$), and then moves away at an interval of 0.5ft till (4,1.5,0)ft as depicted in Fig. 2(b).

Fig. 3 shows the received voltages vs. eavesdropper node positions under both configuration 1 and 2. In Fig. 3(a), received voltages of the legitimate Rx node (denoted by V_{Rx}) and the eavesdropper node (denoted by V_E) are shown against different positions of the eavesdropper node under configuration 1. It can be seen that the legitimate Rx node experiences changes in its received voltage against different positions of the eavesdropper node. It can also be seen that the eavesdropper node itself receives a different voltage at different positions. Maximum voltage received in the eavesdropper node at positions (0,3,0)ft and (0.5,3,0)ft, while minimum voltage received in the eavesdropper node at positions (2,3,0)ft and (2.5,3,0)ft. This means that the position of the eavesdropper node influences the eavesdropping process on the ongoing legitimate MI communication. That is, in some positions, the eavesdropper node may receive maximum information, while in others, it may receive less information due to the low-voltage signal it receives. Furthermore, in this configuration, it is quite possible that the legitimate nodes can sense malicious activities due to the change in the received voltage in the legitimate Rx node and, therefore, can apply countermeasure techniques.

Similarly, Fig. 3(b) shows the voltage received in the legitimate Rx node and eavesdropper node versus different positions of the eavesdropper node based on the configuration 2 setup. The legitimate Rx node exhibits little to no change in the received voltage, as shown in Fig. 3(b). The maximum received voltage in the eavesdropper node in this configuration can be seen in the position (0,1.5,0) feet. This is expected because the eavesdropper node is now half a distance closer to the legitimate Tx node and, therefore, receives a higher voltage than Fig. 3(a) in configuration 1. However, the eavesdropper node received negligible voltage at position (1,1.5,0)ft and may not receive any information at this position from ongoing MI communication.

To conclude, in both configurations 1 and 2, the eavesdropper node can receive information from the ongoing legitimate MI communication. The amount of information the eavesdropper node can get depends on its position with respect to the legitimate Tx node. Furthermore, due to the slight changes in the received voltage of the legitimate Rx node, Rx can detect malicious activity and apply countermeasures accordingly. Therefore, receiver sensitivity and receiver processing capabilities can play an important role.

2) Eavesdropper node orientation: Since the orientation of coils can be changed in the underwater environment due to water movements and tides, it is important to study the impact of the coil orientations on the eavesdropping attack. In addition to the natural changes in the orientation of the coils, the eavesdropper may be smart enough to change its orientation to receive higher voltage and, therefore, eavesdrop more information.

To study the impact of the orientation of the eavesdropper node with respect to legitimate nodes, we consider three different configurations, as shown in Fig. 4. In all three configurations, the legitimate Tx and Rx nodes are kept fixed at a distance of 4ft, with positions (0,0,0)ft and (4,0,0)ft, respectively, unless explicitly mentioned. As legitimate Tx and Rx coils face each other, the angle $\theta_L^{Tx-Rx} = 0°$ receives the maximum signal strength. However, the position

and angle of the eavesdropper node change in a rotational fashion with respect to the legitimate Tx node, the legitimate Rx node, and its own origin, which we model in the following configurations.

3) Configuration 3: In this configuration, the eavesdropper node is initially placed 2ft away from the legitimate Tx node at (-2,0,0)ft (i.e., $d^{Tx-E} = 2ft$), where the angle between them is initially $\theta^{Tx-E} = 0°$. The angle is then rotated at an interval of $\theta = 30°$ from $0°$ to $180°$ around the legitimate Tx node as shown in Fig.4(a).

In Fig. 5, the magnetic flux density is shown based on configuration 3, where the eavesdropper node had a different orientation from the legitimate Tx node. Although there is no significant change in the overall magnetic flux density, the magnetic flux (which is $\phi = BAcos\theta$) would be different in each case of Fig. 5(a), 5(b), and 5(c) because the orientation of the eavesdropper node with respect to the magnetic field lines and magnetic flux density at that position plays a significant role. For the case of Fig. 5(a) and 5(c), the magnetic flux is stronger because the magnetic flux density is relatively high and the magnetic field lines coming toward the eavesdropper node area are with some angle, i.e. $\theta^{Tx-E} \neq 0$. As shown in Fig. 5(b), magnetic flux approaches zero because the magnetic field lines and the coil orientation are parallel to each other, i.e., $\theta^{Tx-E} = 90°$.

Unlike the magnetic flux density results, Fig. 6 illustrates how much voltage can be received by the eavesdropper node due to a different orientation with respect to the legitimate Tx node. Furthermore, the impact of the orientation of the eavesdropper node on the received voltage of the legitimate Rx node must be identified. From Fig. 6, maximum voltage received can be seen at the eavesdropper angles $\theta^{Tx-E} = 0°$, $\theta^{Tx-E} = 30°$, and $\theta^{Tx-E} = 150°$, which shows that the eavesdropper node is approximately face-to-face to the Tx node, and hence will receive maximum information. When the angle of the eavesdropper node to the Tx node becomes orthogonal, that is, $\theta^{Tx-E} = 90°$, no voltage is received at the eavesdropper node, and therefore, no information can be retrieved from ongoing legitimate MI communication. On the other hand, minimal to no change can be seen in the voltage received from the legitimate Rx node, except in $\theta^{Tx-E} = 90°$ and $\theta^{Tx-E} = 180°$. That means a decoupling occurs to some extent between the legitimate nodes due to the existence of the eavesdropper node at these angles. Consequently, legitimate nodes can detect malicious activity resulting from this change in the received voltage.

4) Configuration 4: In this configuration, the eavesdropper node is initially placed 2ft away from the legitimate Rx node at (6,0,0)ft (i.e., $d^{Tx-E} = 6ft$), where, initially, the angle between them $\theta^{Rx-E} = 0°$. We note that the respective angle between legitimate Tx and the eavesdropper node is also initially $\theta^{Tx-E} = 0°$. Then the angle of the eavesdropper node is rotated in an interval of $\theta = 30°$ from $0°$ to $180°$ around the legitimate Rx node as shown in Fig. 4(b).

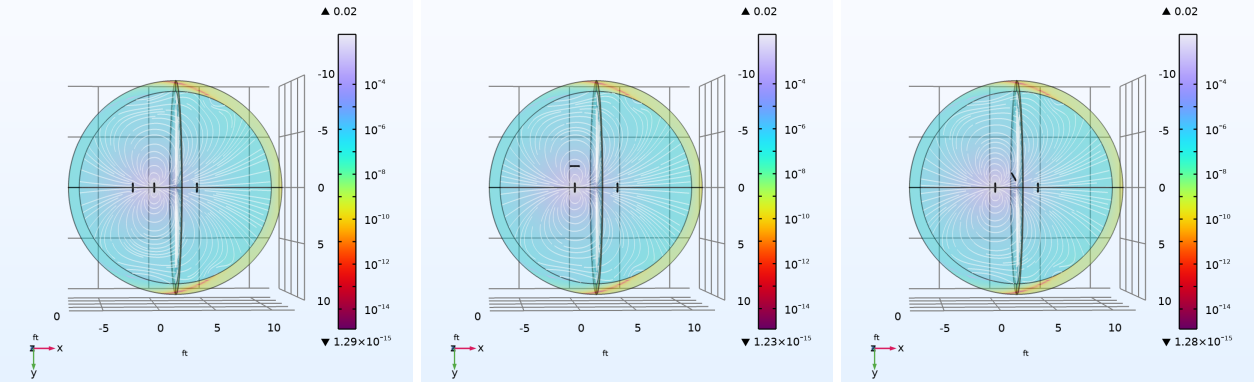
Fig. 7 shows the magnetic flux density based on configuration 4, where the eavesdropper node had a different orientation with respect to the legitimate Rx node instead of a legitimate Tx node. In this case, we note that the eavesdropper node is farther away, i.e., (6,0,0)ft from the legitimate Tx node when its orientation is $\theta^{Rx-E} = 0°$ as shown in Fig. 7(a). Therefore, the magnetic flux density B is weaker, and hence, the magnetic flux is minimal. However, the existence of a legitimate Rx node here may change the magnetic field signal strength and act as a waveguide node, which can either tune or de-tune the magnetic field signal at the eavesdropper node. Fig. 7(b) is a special case because here the orientation of the eavesdropper node and the legitimate Rx node is $\theta^{Rx-E} = 90°$, but it can be seen that the angle between the legitimate Tx node and eavesdropper is not equal to 90 degrees, i.e., $\theta^{Tx-E} \neq 0$. Therefore, the eavesdropper node will receive some magnetic field at this orientation, unlike in the case of Fig. 5(b). In Fig. 7(c), the position of the eavesdropper node is between the legitimate nodes Tx and Rx due to the orientation angle of $\theta^{Rx-E} = 150°$. Although the eavesdropper node is close to the legitimate Tx, however, the angle of magnetic field lines is parallel to the eavesdropper node, and consequently, will receive a lower magnetic flux density and magnetic flux.

Fig. 8 shows the voltage received at the legitimate Rx and eavesdropper nodes based on configuration 4. It can be seen that the eavesdropper node receives the maximum voltage at $\theta^{Rx-E} = 180°$, and hence can get the maximum information from the legitimate communication. The minimum received voltage can be observed at $\theta^{Rx-E} = 0°$, which keep steadily increasing till $\theta^{Rx-E} = 120°$, and then linear increase in voltage is observed from $\theta^{Rx-E} = 120°$ to $\theta^{Rx-E} = 150°$. In the case of a legitimate Rx node, a minimal to no change can be observed against the angles of the eavesdropper node except in $\theta^{Rx-E} = 180°$.

5) Configuration 5: In this configuration, the legitimate nodes Tx and Rx are kept fixed, 2ft apart, at positions (0,0,0)ft and (2,0,0)ft (i.e., $d_L^{Tx-E} = 2ft$). The eavesdropper node is initially placed 2ft away from the legitimate Rx node at position (4,0,0)ft (i.e., $d^{Rx-E} = 2ft$), where the angle between them is $\theta^{Rx-E} = 0°$. Then the angle of the eavesdropper node is changed in a rotational fashion at an interval of $\theta = 15°$ from $0°$ to $180°$ around its own origin, as shown in Fig.4(c).

Fig. 9 shows the magnetic flux density in configuration 5, where the eavesdropper node changes its coil orientation around its own origin. In this configuration, the orientations of $\theta^{Rx-E} = 0°$ and $\theta^{Rx-E} = 180°$ will have similar results since, in both cases, the eavesdropper node faces the legitimate Tx and Rx nodes. When $\theta^{Rx-E} = 150°$, the magnetic flux is lower, since the magnetic field lines and the eavesdropper coil's orientation are nearly parallel to each other. However, when the orientation of the eavesdropper node is orthogonal, i.e. $\theta^{Rx-E} = 90°$ to the legitimate Tx and Rx nodes, it will have zero magnetic flux. Therefore, no magnetic field strength can be received at the eavesdropper node, and consequently, no information can be eavesdropped from the ongoing legitimate MI communication.

The results of the received voltage at the legitimate Rx and eavesdropper nodes based on configuration 5 are shown in Fig. 10, where the eavesdropper node changes orientation around its own origin. It can be seen from the figure that the overall voltage received by the eavesdropper node at this position is minimal. However, the eavesdropper node can



(a) (b) (c)

Fig. 5: Magnetic flux density norm in T with respect to different eavesdropper node angle in the case of configuration 3 when: (**a**) $\theta^{Tx-E} = 0°$, (**b**) $\theta^{Tx-E} = 90°$, and (**c**) $\theta^{Tx-E} = 150°$.

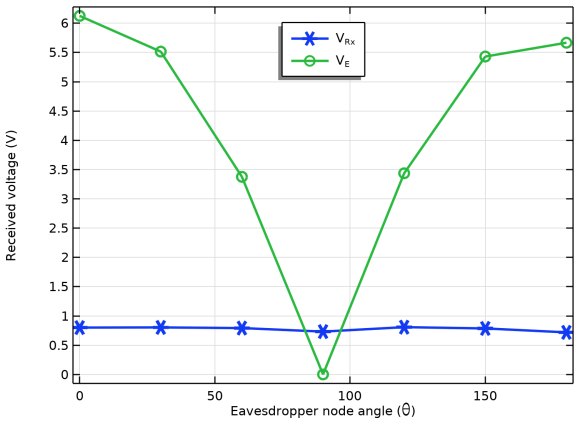


Fig. 6: Received voltage in legitimate Rx node and eavesdropper node vs. different eavesdropper node orientation by changing its angle in a rotational fashion w.r.t. legitimate Tx node position - configuration 3.

receive maximum voltage at $\theta^{Rx-E} = 0°$ and $\theta^{Rx-E} = 180°$. However, the received voltage decreases at other orientations and approaches zero received voltage at $\theta^{Rx-E} = 90°$. On the other hand, slight changes in the received voltages of the legitimate Rx node can be seen against the orientation of the eavesdropper node.

In conclusion, the position of the eavesdropper node and its coil orientation play a significant role in the eavesdropping of legitimate ongoing MI communication. From the results based on Sections III-B1 and III-B2, it can be stated that the eavesdropper node can obtain maximum information from an ongoing legitimate MI communication when the eavesdropper is aligned with and located close to the legitimate position of the Tx node. On the other hand, if the orientation of the eavesdropper node is orthogonal to the Tx node, then it will receive zero information no matter how close it is to the Tx node or the Rx node. In addition, the legitimate node may also sense malicious activities in some eavesdropper position and orientation. However, the legitimate node can sense the change in magnetic flux or received voltage and apply countermeasures to jam the eavesdropper node.

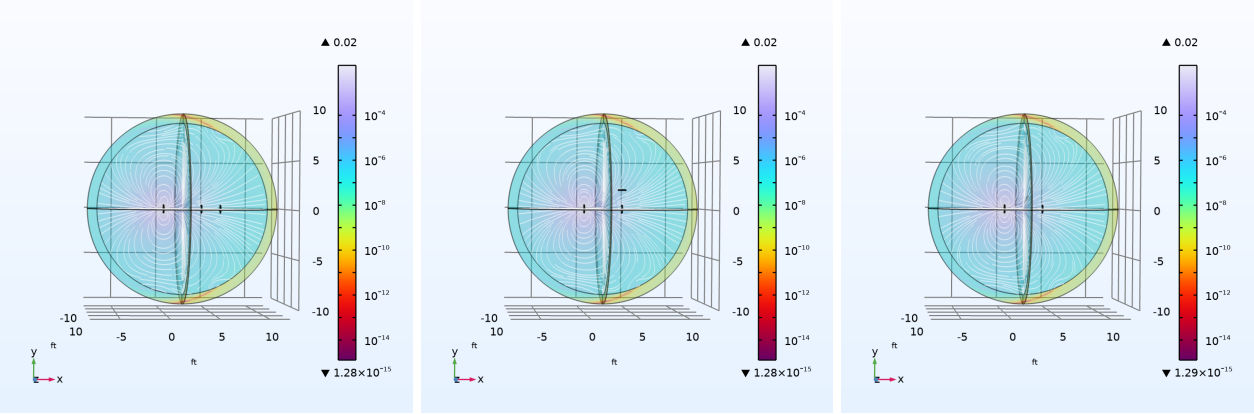
6) Secrecy Capacity Evaluation: In this section, we develop a FEM simulation model of an eavesdropping attack and consider secrecy capacity as the performance metric for evaluation. In this setup, the legitimate Tx node is kept fixed at (0,0,0)ft, while the legitimate Rx node is initially placed at (0.5,0,0)ft and then moved away from the Tx node till (4,0,0)ft at an interval of 0.5ft each time. The eavesdropper node is placed initially at (0,4.5,0)ft and moved away till (0,7.5,0)ft at an interval of 1ft each time.

Fig. 11 shows the secrecy capacity versus the legitimate position of the Rx node for different positions of the eavesdropper node. The maximum secrecy capacity can be observed in Fig. 11 when the eavesdropper position is (0,7.5,0)ft and the minimum secrecy capacity can be seen when the eavesdropper node approaches the legitimate Tx node, i.e., (0,4.5,0)ft. Because, in the considered setup for evaluating the secrecy capacity, the legitimate Tx and Rx nodes are kept fixed and only the eavesdropper node is moved away from the legitimate Tx node in parallel. When the eavesdropper node position is far from the legitimate Tx node, then it receives less voltage, and therefore, the second term in (5) is less prominent than the first term. Consequently, the secrecy capacity will be maximum and vice versa. To conclude, higher secrecy capacity can be achieved when the eavesdropper node is not closer to the legitimate Tx node than the legitimate Rx node. In addition, better secrecy capacity can be achieved when the legitimate Tx and eavesdropper nodes are not aligned to each other, especially when they are orthogonal to each other.

C. Experiments-based Study

We developed a lab experiment to study eavesdropping in MI communication, as shown in Fig. 12. To compare the results of the FEM simulation and the experimental test setup, we used similar parameters and the same configurations as described in Section III.

In the lab setup, the parameters used in the simulation setup (listed in Table. I) are kept the same, except for the coils'



(a) (b) (c)

Fig. 7: Magnetic flux density norm in T with respect to different eavesdropper node angle in the case of configuration 4 when: (**a**) $\theta^{Rx-E} = 0°$, (**b**) $\theta^{Rx-E} = 90°$, and (**c**) $\theta^{Rx-E} = 150°$.

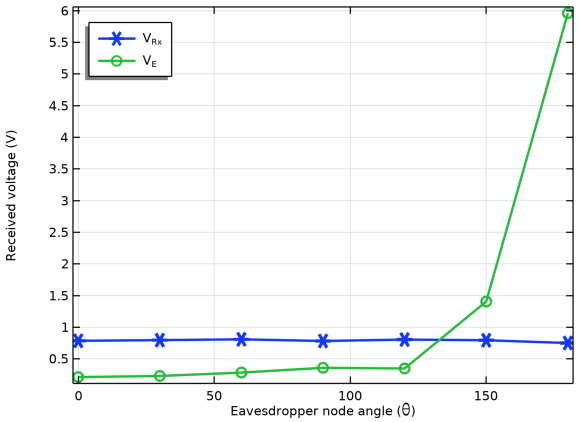


Fig. 8: Received voltage in legitimate Rx node and eavesdropper node vs. different eavesdropper node orientation by changing its angle in a rotational fashion w.r.t. legitimate Rx node position - configuration 4.

TABLE II: Capacitors and coils inductance value used in the experimental setup.

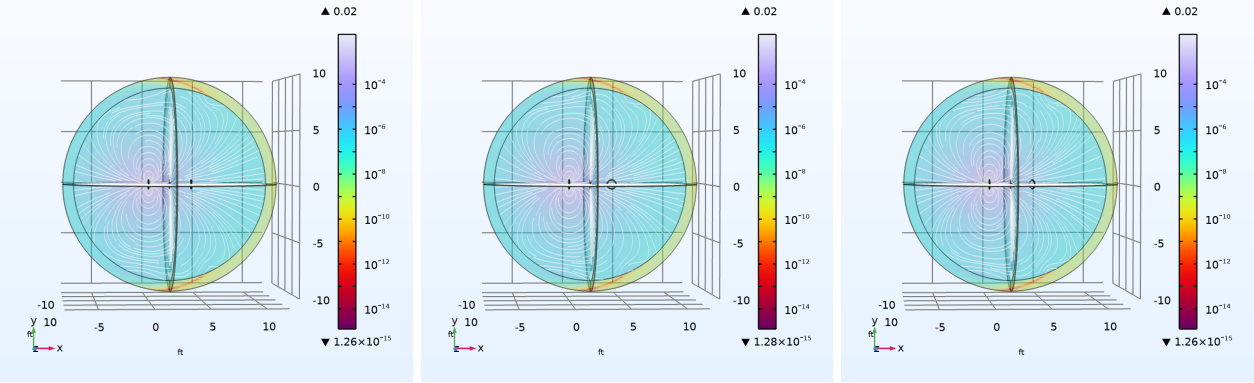
	Tx node	Rx node	Eavesdropper node
Capacitance	5.62 nF	5.62nF	5.62 nF
Inductance	449 μH	447 μH	446 μH

inductance and capacitance. The capacitance and inductance of the legitimate Tx, Rx, and eavesdropper node are given in Table II. The legitimate Tx is excited with a sinusoidal voltage signal of $10V$ from the waveform generator. The signals from the legitimate Rx node and the eavesdropper node are recorded from the oscilloscope.

Fig. 13 shows experimental results of received voltage versus eavesdropper node position (discussed in section III-B1) under configurations 1 and 2, respectively (shown in Fig.2). Fig.13(a) shows the voltage received at the legitimate Rx and eavesdropper nodes vs. different positions of the eavesdropper nodes based on the configuration 1 setup. A similar trend can be seen here compared to the simulation results shown in Fig. 3(a). The received voltage at the eavesdropper node changes based on its different position with respect to the legitimate nodes. Similarly, minimal changes in the received voltage of legitimate Rx nodes can be observed against different eavesdropper positions.

The results of the experimental setup based on configuration 2 discussed in Section III-B1 are shown in Fig. 13(b). In this configuration, the eavesdropper node approaches the Tx node, and the maximum voltage is received at the eavesdropper node at position (0,1.5,0)ft. While a change in the received voltage of the eavesdropper node can be observed at different positions of the eavesdropper node between legitimate Tx and Rx nodes, minimal to no change can be seen in the legitimate node voltage received. To summarize the results of Fig. 13, the eavesdropper node may obtain maximum or minimum information from the ongoing legitimate communication based on its position in the vicinity of the ongoing legitimate MI communication.

Fig. 14 shows the voltages received at the legitimate Rx and eavesdropper nodes vs. different angles of the eavesdropper nodes based on the experimental lab setup. The subfigure in Fig. 14 shows the experimental results for the three different configurations as discussed in Section III-B2. The difference between the simulation setup and the experimental setup is that the angle of the eavesdropper node changes at an interval of $\theta = 30°$ in the case of the experimental setup. From Fig. 14(a), it can be seen that the eavesdropper node can receive maximum voltage when the Tx node and the eavesdropper node are facing each other, i.e. $\theta^{Tx-E} = 0°$ or $\theta^{Tx-E} = 180°$, while the eavesdropper node receives zero voltage at $\theta^{Tx-E} = 90°$. On the other hand, the voltage received in the legitimate Rx node shows a significant change at $\theta^{Tx-E} = 90°$, otherwise a minimal to no change can be observed. From Fig. 14(b), it can be seen that the eavesdropper node receives minimal to no voltage until the angle of the eavesdropper node is greater than $120°$. In this case, minimal to no change in voltage can be observed at the legitimate Rx node. In Figure 14(c), it can be seen that the voltage received in the eavesdropper node is generally minimal, while it approaches zero at an angle of



(a) (b) (c)

Fig. 9: Magnetic flux density norm in T with respect to different eavesdropper node angle in the case of configuration 5 when: (**a**) $\theta^E = 0°$, (**b**) $\theta^E = 90°$, and (**c**) $\theta^E = 150°$.

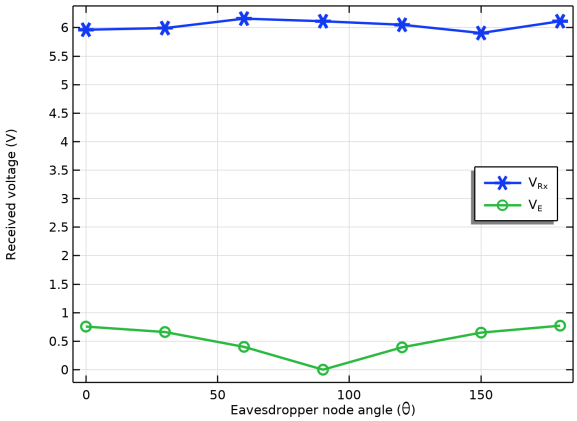


Fig. 10: Received voltage in legitimate Rx node and eavesdropper node vs. different eavesdropper node orientation by changing its angle in a rotational fashion w.r.t. its own origin - configuration 5.

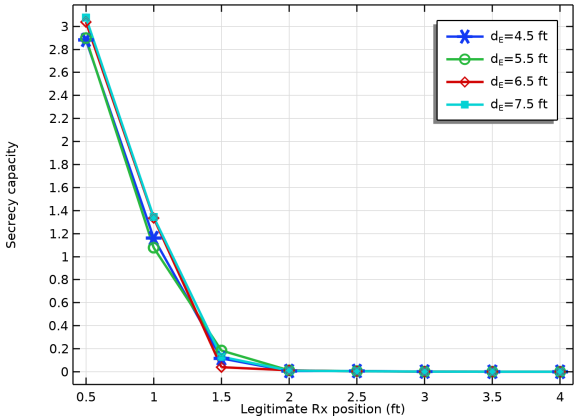


Fig. 11: Secrecy capacity vs. legitimate node position under different eavesdropper node positions.

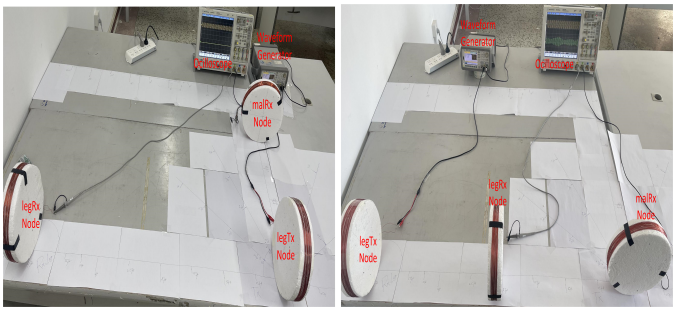


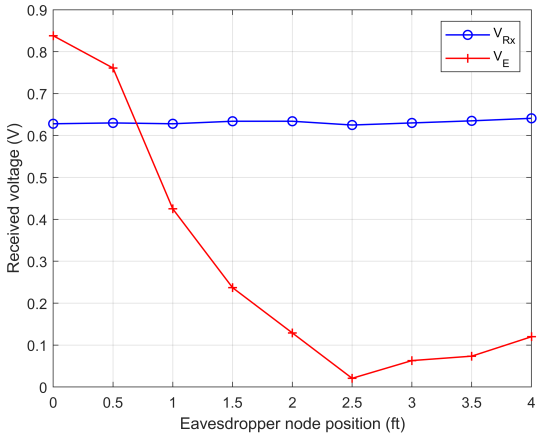
Fig. 12: A glance of an experimental lab setup.

$\theta^{Rx-E} = 90°$. The voltage received at the legitimate Rx node shows slight changes, specifically at $\theta^{Rx-E} = 90°$.

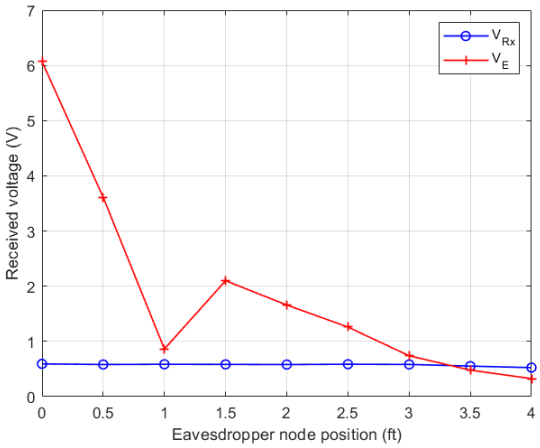
In summary, the results achieved from the experimental tests exhibit trends that are almost similar for each configuration to those obtained in the FEM-based simulation results. Results from both the FEM simulation and experimental tests verify that the eavesdropper can eavesdrop on the ongoing legitimate MI communication, but this depends on the eavesdropper's position and orientation with respect to legitimate nodes. Furthermore, legitimate nodes may detect malicious activities in the vicinity due to changes in the MI signal strength/received voltage at the legitimate Rx node.

IV. Conclusion

In this paper we present a detailed investigation of the vulnerability of underwater MI communication to eavesdropping attacks. We consider a scenario with three MI nodes: legitimate Tx and Rx nodes, and an eavesdropper node, and answer the following questions: 1) can an eavesdropper eavesdrop on legitimate MI communication and 2) can legitimate nodes sense the malicious activity of the eavesdropper node. For this, we conducted FEM simulations and laboratory experiments. The results show that underwater MI communication systems are indeed vulnerable to eavesdropping attacks, showing that an eavesdropper can eavesdrop on underwater MI-based legitimate communication, mainly based on the position and



(a)



(b)

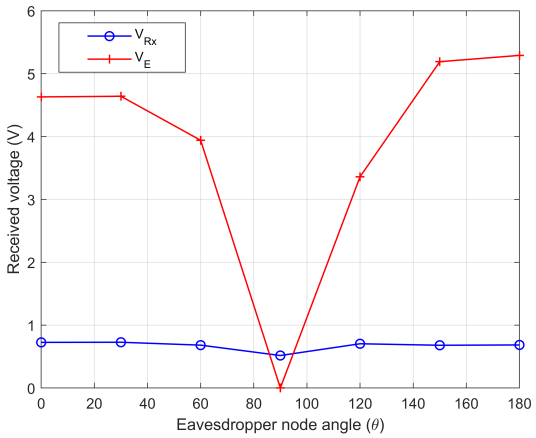
Fig. 13: Experimental results based on eavesdropper node position with respect to legitimate Tx and Rx positions: (**a**) Received voltage vs. eavesdropper node position under Configuration 1 and (**b**) Received voltage vs. eavesdropper node position under configuration 2.

orientation of the eavesdropper node with respect to legitimate nodes. The results also show that legitimate nodes might be able to detect malicious activities based on the eavesdropper's position and orientation.

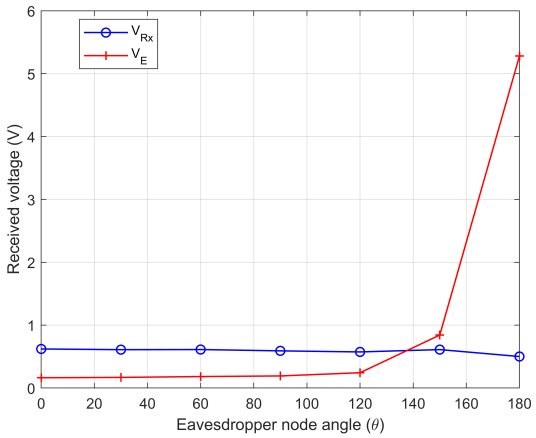
Potential future extensions to this work include: developing a systematic mechanism that can detect eavesdropping from variations in received signals at legitimate coil reception, enhancing the secrecy capacity of the system through resource optimization, and studying the impact of multiple malicious coils present in the surroundings on the information exchange of legitimate coils.

REFERENCES

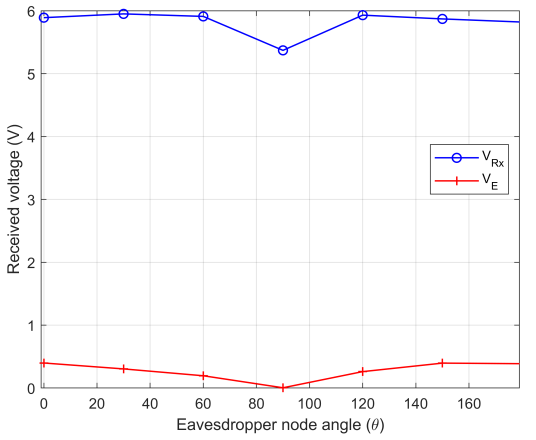
[1] Y. Li, S. Wang, C. Jin, Y. Zhang, and T. Jiang, "A survey of underwater magnetic induction communications: Fundamental issues, recent advances, and challenges," *IEEE Communications Surveys & Tutorials*, 2019.



(a)



(b)



(c)

Fig. 14: Experimental setup based received voltage in legitimate Rx node and eavesdropper node vs. different eavesdropper node orientation by changing its angle (**a**) in a rotational fashion w.r.t. legitimate Tx node position - configuration 3, (**b**) in a rotational fashion w.r.t. legitimate Rx node position - configuration 4, and (**c**) in a rotational fashion w.r.t. its own origin - configuration 5.

[2] M. Muzzammil, N. Ahmed, G. Qiao, I. Ullah, and L. Wan, "Fundamentals and advancements of magnetic field communication for underwater wireless sensor networks," *IEEE Transactions on Antennas and Propagation*, 2020.

[3] M. F. Ali, D. N. K. Jayakody, Y. A. Chursin, S. Affes, and S. Dmitry, "Recent advances and future directions on underwater wireless communications," *Archives of Computational Methods in Engineering*, vol. 27, pp. 1379–1412, 2020.

[4] M. Muzzammil, N. Kouzayha, N. Saeed, and T. Y. Al-Naffouri, "Towards sustainable internet of underwater things: UAV-aided energy efficient wake-up solutions," *arXiv preprint arXiv:2208.12065*, 2022.

[5] C. M. Gussen, P. S. Diniz, M. L. Campos, W. A. Martins, F. M. Costa, and J. N. Gois, "A survey of underwater wireless communication technologies," *J. Commun. Inf. Sys*, vol. 31, no. 1, pp. 242–255, 2016.

[6] W. Aman, S. Al-Kuwari, M. Muzzammil, M. M. U. Rahman, and A. Kumar, "Security of underwater and air–water wireless communication: State-of-the-art, challenges and outlook," *Ad Hoc Networks*, vol. 142, p. 103114, 2023.

[7] L. Wan, H. Jia, F. Zhou, M. Muzzammil, T. Li, and Y. Huang, "Fine doppler scale estimations for an underwater acoustic CP-OFDM system," *Signal Processing*, vol. 170, p. 107439, 2020.

[8] Z. Zeng, S. Fu, H. Zhang, Y. Dong, and J. Cheng, "A survey of underwater optical wireless communications," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 204–238, 2017.

[9] I. F. Akyildiz, P. Wang, and Z. Sun, "Realizing underwater communication through magnetic induction," *IEEE Communications Magazine*, vol. 53, no. 11, pp. 42–48, 2015.

[10] M. Muzzammil, Z. Babar, N. Ahmed, G. Qiao, and S. Liu, "Directivity pattern of different coil structures for magneto-coupled communication systems," in *OCEANS 2019-Marseille*. IEEE, 2019, pp. 1–4.

[11] W. Aman, M. M. Rahman, Z. Haider, J. Qadir, M. W. Nawaz, and G. A. Sidhu, "Maximizing secrecy rate of an orthogonal frequency division multiplexing-based multihop underwater acoustic sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 11, p. e4106, 2020.

[12] Q. Wang, H.-N. Dai, X. Li, H. Wang, and H. Xiao, "On modeling eavesdropping attacks in underwater acoustic sensor networks," *Sensors*, vol. 16, no. 5, p. 721, 2016.

[13] S. Jiang, "On securing underwater acoustic networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 729–752, 2018.

[14] I. Ahmad, T. Rahman, A. Zeb, I. Khan, I. Ullah, H. Hamam, and O. Cheikhrouhou, "Analysis of security attacks and taxonomy in underwater wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 2021, no. 1, p. 1444024, 2021.

[15] M. Kong, J. Wang, Y. Chen, T. Ali, R. Sarwar, Y. Qiu, S. Wang, J. Han, and J. Xu, "Security weaknesses of underwater wireless optical communication," *Optics Express*, vol. 25, no. 18, pp. 21 509–21 518, 2017.

[16] X. Zhang, G. Klevering, X. Lei, Y. Hu, L. Xiao, and G.-H. Tu, "The security in optical wireless communication: A survey," *ACM Computing Surveys*, vol. 55, no. 14s, pp. 1–36, 2023.

[17] R. Boluda-Ruiz, P. Salcedo-Serrano, B. Castillo-Vázquez, A. García-Zambrana, and J. M. Garrido-Balsells, "Impact of scattering on secrecy outage probability of underwater optical wireless links," *IEEE Journal of Oceanic Engineering*, 2023.

[18] D. Nelson, M. Qiao, and A. Carpenter, "Security of the near field communication protocol: an overview," *Journal of Computing Sciences in Colleges*, vol. 29, no. 2, pp. 94–104, 2013.

[19] M. RAHMAN and H. ELMILIGI, "Classification and analysis of security attacks in near field communication," *International Journal of Business and Cyber Security*, vol. 1, no. 2, 2017.

[20] H. Sun, H. Lin, F. Zhu, and F. Gao, "Magnetic resonant beamforming for secured wireless power transfer," *IEEE Signal Processing Letters*, vol. 24, no. 8, pp. 1173–1177, 2017.

[21] A. A. Al Islam, T. Chakraborty, T. A. Khan, M. Zoraf, and C. S. Hyder, "Towards defending eavesdropping on NFC," *Journal of Network and Computer Applications*, vol. 100, pp. 11–23, 2017.

[22] M. M. Singh, K. Adzman, and R. Hassan, "Near field communication (NFC) technology security vulnerabilities and countermeasures," *International Journal of Engineering & Technology*, vol. 7, no. 4.31, pp. 298–305, 2018.

[23] A. H. Alrobaish, W. F. Al-mutairi, H. A. Alsuqayhi, and D. M. Ibrahim, "Common attacks on near field communication technology," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*. IEEE, 2022, pp. 110–114.

[24] S. Han, H.-J. Kim, J. Lee, and J.-W. Choi, "Secure capacity analysis for magnetic inductive coupling-based swipt system," *IEEE Access*, vol. 6, pp. 49 182–49 191, 2018.

[25] S. P. Ravindran, J.-F. Bousquet, and N. Gaoding, "Characterization of a 3d underwater magneto-inductive transmitter coil array," in *OCEANS 2018 MTS/IEEE Charleston*. IEEE, 2018, pp. 1–6.

[26] M. Hott and P. A. Hoeher, "Underwater communication employing high-sensitive magnetic field detectors," *IEEE Access*, vol. 8, pp. 177 385–177 394, 2020.

[27] N. Ahmed, A. Radchenko, D. Pommerenke, and Y. R. Zheng, "Design and evaluation of low-cost and energy-efficient magneto-inductive sensor nodes for wireless sensor networks," *IEEE Systems Journal*, no. 99, pp. 1–10, 2018.

[28] J. I. Agbinya and M. Masihpour, "Power equations and capacity performance of magnetic induction communication systems," *Wireless Personal Communications*, vol. 64, pp. 831–845, 2012.

[29] M. C. Domingo, "Magnetic induction for underwater wireless communication networks," *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 6, pp. 2929–2939, 2012.

[30] D. Wei, L. Yan, C. Huang, J. Wang, J. Chen, M. Pan, and Y. Fang, "Dynamic magnetic induction wireless communications for autonomous-underwater-vehicle-assisted underwater IoT," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 9834–9845, 2020.