Spoofing Detection Games in Underwater Sensor Networks

Yan Li, Liang Xiao*, Qiangda Li, Wei Su

*Dept. of Communication Engineering, Xiamen University, Xiamen, China. Email: lxiao@xmu.edu.cn

***Abstract*—Spoofing detection is essential in underwater sensor networks (UWSNs), especially for safety-critical applications. Because of the high bit error rates, low bandwidth and large delay of the acoustic channels, it is challenging to detect spoofing attacks in UWSNs. In this paper, we propose spoofing detection strategies based on reinforcement learning. The interactions between a surface station and an underwater spoofer are formulated as a zero-sum game. The Nash equilibrium (NE) of the spoofing detection game in UWSNs is derived and the existing condition for a unique NE is provided. A spoofing detection method based on Q-learning is proposed for dynamic underwater sensor networks. Simulation results have validated the efficacy of the proposed spoofing detection scheme in UWSNs.**

I. Introduction

Spoofing detection is essential in underwater sensor networks (UWSNs), especially for safety-critical applications [1]–[3]. By claiming to be another underwater sensor with faked MAC addresses, spoofing attackers can obtain illegal advantages and further perform other types of attacks such as man-in-the-middle attacks and denial-of-service attacks [4].

Traditional authentication techniques that mostly focus on Internet or wireless networks, such as digital signature [5], have been commonly adopted to address spoofing attacks. As complement of traditional security mechanisms, PHY-layer authentication techniques [6]–[10] have been proposed, which exploit the unique properties of transmitters and channels such as received signal strength [6] to detect spoofing attacks in wireless networks. However, due to the severe attenuations, large delay, severe multipath and narrow bandwidth of underwater acoustic propagations, it is difficulty to fully address spoofing attacks in UWSNs.

In this paper, we investigate the authentication in UWSNs and build a hypothesis test to detect spoofing attacks in UWSNs. We consider an underwater sensor network consisting of several sensors at various locations and a sink in a boat slowly floating in the area. By applying traditional higher-layer authentication technique or PHY-layer authentication techniques, the surface sink detects spoofing attacks thrown by an underwater transmitter by comparing the digital signatures or channel characteristics variance with a test threshold.

The interactions between the surface sink and an underwater spoofer are formulated as a zero-sum spoofing detection game in UWSNs. Once collecting data from the sensors over underwater acoustic channels, the surface sink chooses its test threshold in the hypothesis test to detect spoofing, while the spoofer determines its attack frequency, i.e., the frequency to send spoofing data. Both the spoofer and the surface sink are assumed to autonomously choose their actions to maximize their individual expected utility in the spoofing detection. Nash equilibrium (NE) in the spoofing detection game is derived and its uniqueness is discussed. Both the optimal strategies of the players in the NE are based on the spoofing cost and the weight factor, which measures the impacts of the gain of accepting a legitimate packet and that of rejecting a spoofing one.

As sensors float randomly in the area over time, it is challenging for a surface sink to choose a proper test threshold in the authentication. Therefore, we propose a spoofing detection scheme based on reinforcement learning for a sink with unknown parameters in dynamic underwater environments. The optimal test threshold in the spoofing detection is achieved by learning from the spoofing detection history. Simulations in various underwater sensor network scenarios are performed to evaluate the efficiency of the proposed spoofing detection scheme. Simulation results demonstrate that the proposed spoofing detection method can efficiently improve the spoofing detection accuracy and the utility of UWSNs.

The main contributions of the paper lie in three aspects: 1) We propose an authentication scheme that applies the hypothesis test to detect spoofing attacks in UWSNs. 2) The interactions between an underwater spoofer and a surface sink are formulated as a zero-sum game. The unique NE of the game is derived and its uniqueness is discussed. 3) The spoofing detection based on reinforcement learning is proposed for dynamic UWSNs with unknown parameters such as the opponent's strategy. The performance of the proposed spoofing detection scheme is evaluated via simulations.

The remainder of the paper is organized as follows. We review related work in Section II. In Section III, we present the system model and the spoofing detection game. A reinforcement learning-based spoofing detection scheme is presented in Section IV. We provide simulation results in Section V and conclude in Section VI.

This work was supported in part by NSFC (No. 61271242, 61301097, 61440002) and the Fundamental Research Funds for the Central Universities (2013121023).

This is a DRAFT. As such it may not be cited in other works. The citable Proceedings of the Conference will be published in IEEE Xplore shortly after the conclusion of the conference.

978-0-933957-43-5 ©2015 MTS

II. Related Work

Due to the characteristics of the acoustic channels, underwater sensor networks are vulnerable to attacks. Security in UWSNs was discussed in [1], showing that spoofing attacks can be detected by encryptions of all packets. State information of nodes was applied in [11] to detect Sybil attacks in UWSNs. The power consumptions of different digital signature schemes was evaluated for end-to-end authentication in UWSNs in [12].

Several PHY-layer authentication techniques have been proposed to detect spoofing attacks in wireless networks. For instance, spoofing detection was developed based on the spatial correlation of received signal strength instead of the digital signatures in traditional authentication [6]. Channel impulse responses were explored in physical layer authentication for multipath propogation wireless environments [7]. In [9], machine learning such as support vector machine was used to detect spoofing by utilizing channel state information. In [13], a PHY-layer spoofing detector with test threshold chosen based on learning was proposed in dynamic wireless networks.

In this work, we apply the reinforcement learning technique to detect spoofing attacks for surface stations and use game theory to investigate the spoofing detection process of underwater sensor networks.

III. System model & game formulation

We consider an underwater sensor network that consists of a surface station or sink, N underwater sensor transmitters and an underwater spoofer which can impersonate another node to perform spoofing attacks, as shown in Fig. 1. The underwater sensors use acoustic channels to report the sensing data to surface station. The probability of the spoofer to send a spoofing packet is denoted by $y \in [0,1]$. The surface station can apply a conventional authentication based on digital signatures in [5] or PHY-layer authentication with channel transfer functions in UWSNs in [8] to detect spoofing.

The distance between sensor i and the surface station is denoted by d_i. Based on [14] and the Thorp's formula, the acoustic path loss between the surface station and sensor i at the acoustic signal frequency f is given by

$$A(d_i, f) = h_0 d_i^{\gamma} \alpha(f)^{d_i} \tag{1}$$

$$\alpha(f) = 10^{\frac{0.011 f^2}{1+f^2} + \frac{4.4 f^2}{4100+f^2} + 2.75\times 10^{-5} f^2 + 3\times 10^{-4}}, \tag{2}$$

where γ is the path loss exponent for spherical spreading, h_0 is the reference path loss, and $\alpha(f)$ is the absorption coefficient.

Assume that the surface station receives packets from M acoustic paths, with the length of the m-th path denoted by l_m. The additional loss on the m-th path is denoted by κ_m. By [14], the channel transfer function of sensor i with the M paths is given by

$$H_i(f) = \sum_{m=0}^{M-1} \frac{\kappa_m e^{-j2\pi f l_m / c}}{\sqrt{A(l_m, f)}}, \tag{3}$$

where $c = 1500$ mps is the nominal underwater sound speed.

Based on the uniqueness of acoustic channels, the surface station can discriminate sensors at different locations by their channel transfer functions. If the channel transfer function of sensor i and its reference channel transfer function which stored by the surface station in advance are very different, the message is spoofing. Otherwise, the message is legitimate.

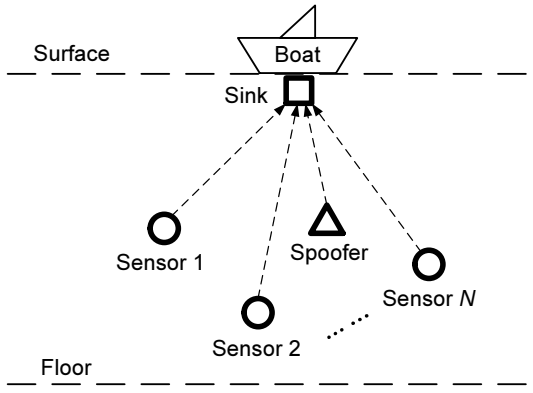


Fig. 1. Anti-spoofing game of an underwater sensor network with N acoustic sensors and a spoofer.

In the traditional digital signature-based authentication or the PHY-layer authentication, a hypothesis test is built by the surface station to determine whether a packet indeed comes from the claimed transmitter. Without loss of generality, the packet claiming to be sent by sensor i is denoted by Γ_i. The null hypothesis $\mathcal{H}_0$ indicates that the packet Γ_i is indeed sent by sensor i. The alternative hypothesis $\mathcal{H}_1$ indicates that packet Γ_i is sent by the spoofer. The hypothesis test of the spoofing detection for UWSNs is given by

$$\mathcal{H}_0 : h(\Gamma_i) = i \tag{4}$$

$$\mathcal{H}_1 : h(\Gamma_i) \neq i, \tag{5}$$

where $h(M)$ represents the real sender of the message.

The test statistic of the hypothesis test, denoted by $L \in [0,1]$, can be extracted from the packet, e.g., the normalized variance of the digital signatures or the channel characteristics. Let $x \in [0,1]$ be the normalized test threshold in the authentication. If the test statistic is small than the test threshold x, the surface station accepts the null hypothesis $\mathcal{H}_0$. In other hand, $\mathcal{H}_1$ is accepted. Then the hypothesis test is given by

$$L \underset{\mathcal{H}_1}{\overset{\mathcal{H}_0}{\lessgtr}} x. \tag{6}$$

The false alarm rate of the spoofing detection is the probability that a legitimate packet is classified as a spoofing packet, while the miss detection rate is the probability that a spoofing packet is classified as a legitimate packet. Both of them depend on the threshold x of the surface station. By definition, the false alarm rate and the miss detection rate, denoted by $f(x)$ and $g(x)$, respectively, are given by

$$f(x) = \Pr(\mathcal{H}_1 | \mathcal{H}_0) \tag{7}$$

$$g(x) = \Pr(\mathcal{H}_0 | \mathcal{H}_1). \tag{8}$$

It is clear that $f(0) = 1$, $f(1) = 0$, $g(0) = 0$ and $g(1) = 1$. We also have $f(x)$ decreases with x, while $g(x)$ increases with it.

The interactions between the surface station and the spoofer can be formulated as a zero-sum authentication game, denoted by $\mathbf{G}$. In this game, the surface station chooses its test threshold x of the authentication, while the spoofer chooses its spoofing probability y. The spoofing cost of the spoofer is denoted by C. As the surface station aims to detect spoofing attacks, its utility (or that of the spoofer), denoted by U_B (or U_E) is defined as

$$\begin{aligned} U_B(x,y) &= -U_E(x,y) \\ &= (1-f(x))(1-y) + \delta\,(1-g(x))\,y + Cy, \end{aligned} \quad (9)$$

where $\delta \in [0,1]$ is the weight factor between the miss detection and the false alarm. It is clear by definition that $1-f(x)$ is the probability for the surface station to accept a legitimate packet and $1-g(x)$ is the probability to reject a spoofing packet.

The Nash equilibrium of the game is denoted by (x^*, y^*), consisting of the best response strategies, i.e., each player chooses its best response to maximize its utility given that its opponent takes the NE strategy. Thus we have

$$x^* = \arg\max_{0\le x\le 1} U_B(x, y^*) \quad (10)$$

$$y^* = \arg\max_{0\le y\le 1} U_E(x^*, y). \quad (11)$$

To investigate the NE in the spoofing detection game, we use a quadratic model to characterize the false alarm rate, $f(x)$, and the miss detection rate, $g(x)$. It is clear that the false alarm rate decreases with the test threshold, while the miss detection rate increases with it. In addition, $f(0) = 1$, and $f(1) = 0$. For simplicity, the false alarm rate is defined as

$$f(x) = (1-x)^2. \quad (12)$$

Similarly, we have $g(0) = 0$, and $g(1) = 1$, and define the miss detection rate as

$$g(x) = x^2. \quad (13)$$

If both the surface station and the spoofer know all the parameters in the game, the NE of the static spoofing detection game is given by the following:

Lemma 1. *The spoofing detection game* $\mathbf{G}$ *has a unique Nash equilibrium, which is given by*

$$(x^*, y^*) = \begin{cases} (1,0), & C > 1 \\ \left(\frac{1+C}{2}, \frac{1-C}{2}\right), & \delta = 1, C \le 1\,, \\ (\hat{x}, \hat{y})\,, & \delta \ne 1, C \le 1 \end{cases} \quad (14)$$

where $\hat{x} = \frac{\sqrt{1+(\delta-1)(\delta+C)}-1}{\delta-1}$ *and* $\hat{y} = \frac{\sqrt{1+(\delta-1)(\delta+C)}-\delta}{(1-\delta)\sqrt{1+(\delta-1)(\delta+C)}}$.

Proof: See Appendix A. ∎

According to Lemma 1, NE of the game depends on the spoofing cost C and the weight factor δ in (9). The spoofer obtains low benefit under high spoofing cost (i.e., $C > 1$) and thus the optimal strategy is to stop attacking. Correspondingly, the optimal threshold of the surface station is 1 to avoid rejecting legitimate packets. If $\delta = 1$, i.e., the same weight between the gain of rejecting a spoofing packet and that of accepting a legitimate packet, and $C \le 1$, the optimal strategy of the spoofer decreases with the spoofing cost C, while the optimal threshold of the surface station increases with it. Otherwise, if $\delta \ne 1$ and $C \le 1$, both the optimal strategies of the spoofer and the surface station are adjusting their strategies based on δ and C.

IV. Learning-based Spoofing Detection For UWSNs

The repeated interactions between the surface station and spoofer repeat in dynamic underwater sensor networks with both players being unaware of parameters such as the spoofing cost and the opponent's strategy. For instance, as the state of the channel is intensely varied, the surface station has difficulty estimating the characteristics of the packets and calculating its optimal test threshold x in the spoofing detection. Therefore, reinforcement learning such as Q-learning can be applied by the surface station to determine the test threshold by observing the channel environment and packet's characteristics and trials.

Without loss of generality, the surface station quantizes its test threshold x in the spoofing detection into K levels and chooses its threshold from the action set denoted by $\mathbf{A} = [x_a]_{1\le a\le K}$, where $0 \le x_a \le 1$ is the a-th available test threshold. The state of the surface station, denoted by $\mathbf{s}^k$, consists of the false alarm rate and the miss detection rate in the last time slot, i.e., $\mathbf{s}^k = [f^{k-1}(x), g^{k-1}(x)]$, where both $f(x)$ and $g(x)$ are quantized respectively to X levels. At time k, the probability of the spoofer to execute a spoofing attack is denoted by y^k. The instantaneous utility of the surface station at time k, denoted by U_B^k, is given by Eq. (9).

In the spoofing detection, $Q(\mathbf{s}, \mathbf{x})$ denotes the Q function for state $\mathbf{s}$ and test threshold x, while $V(\mathbf{s})$ is the highest Q value of state $\mathbf{s}$. The surface station updates its Q and V functions in each time slot by the following:

$$Q(\mathbf{s}^k, x^k) \leftarrow (1-\alpha)Q(\mathbf{s}^k, x^k) + \alpha(u_B^k + \beta V(\mathbf{s}^{k+1})) \quad (15)$$

$$V(\mathbf{s}^k) \leftarrow \max_x Q(\mathbf{s}^k, x), \quad (16)$$

where α is the learning rate and β is the discount factor, with $0 \le \alpha, \beta \le 1$.

The surface station applies the ϵ-greedy policy to choose the optimal test threshold, i.e., the test threshold x is given by the following probability distribution function,

$$\Pr(x^k = \eta) = \begin{cases} 1-\epsilon, & \eta = \arg\max_{x'\in\mathbf{A}} Q(\mathbf{s}^k, x') \\ \frac{\epsilon}{K-1}, & \eta \in \mathbf{A}, \eta \ne \arg\max_{x'\in\mathbf{A}} Q(\mathbf{s}^k, x') \end{cases}. \quad (17)$$

The spoofing detection of the surface station is summarized in Algorithm 1.

V. Simulation Results

The performance of the proposed spoofing detection was evaluated via simulations with $C = 0.6$, $\alpha = 0.7$, $\beta = 0.9$ and $\epsilon = 0.05$. We assumed that the impacts of the gain of

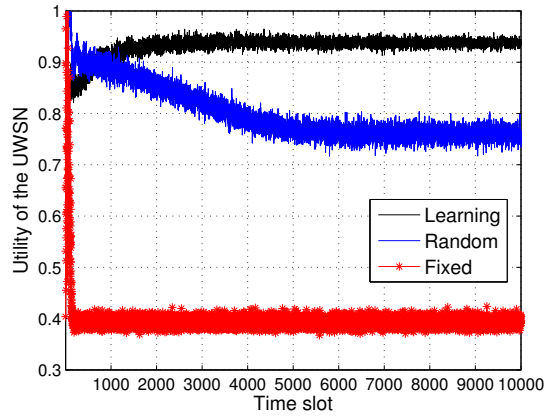
Algorithm 1 Spoofing detection strategy with Q-learning.

1: **Initialize:** α, β, ϵ, $\mathbf{A}$, $Q(\mathbf{s}, x) = 0$, $V(\mathbf{s}) = 0$, $\forall \mathbf{s}, x \in \mathbf{A}$
2: **for** $k = 1, 2, 3, ...$ **do**
3: Observe the current state $\mathbf{s}^k$
4: Select and perform a test threshold $x^k \in \mathbf{A}$ via (17)
5: Observe the subsequent state $\mathbf{s}^{k+1}$ and immediate payoff U_B^k
6: Update $Q(\mathbf{s}^k, x^k)$ via (15)
7: Update $V(\mathbf{s}^k)$ via (16)
8: **end for**

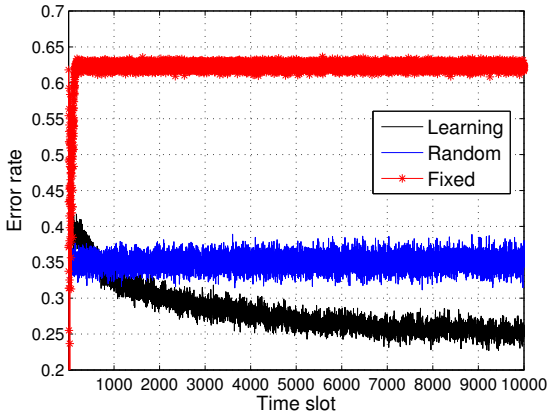
accepting a legitimate packet and that of rejecting a spoofing one were same, i.e., $\delta = 1$. The threshold set of the detection and the probability set of the spoofing were evenly quantized into 11 levels. As benchmark, we considered a random and fixed detection scheme against a smart spoofer that applies Q-learning to choose its spoofing frequency.

As the surface station with the proposed spoofing detection scheme chooses its test threshold according to the environmental change, it receives a higher utility than that with random or fixed strategy (i.e., the test threshold is 0.2), as shown in Fig. 2 (a). For example, if the spoofing cost is 0.6 and the weight factor is 1, after 8000 time slots, the utility of the surface station with the threshold strategy based on Q-learning increases by about 23.7% than that with the random strategy and about 141% than that with the fixed strategy.

As shown in Fig. 2 (b), total error rate of the proposed spoofing detection scheme (i.e., the sum of the false alarm rate and the miss detection rate), is lower than that with the random strategy and the fixed strategy. For example, if the spoofing cost is 0.6 and the weight factor is 1, after 8000 time slots, the error rate achieved by its strategy is 25%, while the random strategy and the fixed strategy are 36% and 63%, respectively.



(a) Utility of the surface station.



(b) Error rate of the spoofing detection.

Fig. 2. Performance of the spoofing detection in dynamic UWSNs with $C = 0.6$, $\delta = 1$, $\alpha = 0.7$, $\beta = 0.9$ and $\epsilon = 0.05$.

VI. Conclude

In this work, we have investigated the authentication process in underwater sensor networks and built hypothesis tests to detect spoofing attacks. The interactions between a surface station and a spoofer in UWSNs were formulated as a zero-sum authentication game. The NE of the static spoofing detection game was investigated, and the conditions were provided. The spoofing detecting based on Q-learning was proposed for surface stations to improve their detection accuracies in dynamic underwater environments with unknown system parameters. As shown in simulation results, the proposed learning-based scheme enhances the detection performance, e.g., the utility of the surface station is 23.7% higher than that with a random test threshold and the error rate is 11% lower, if the spoofing cost is 0.6 and the weight factor is 1.

Appendix A
Proof of **Lemma 1**

By (12) and (13), the utility function in (9) becomes

$$U_B(x,y) = -U_E(x,y) = (2x - x^2)(1-y) + \delta\left(1 - x^2\right) y + Cy, \quad (18)$$

and thus

$$\frac{\partial U_B(x,y)}{\partial x} = 2 - 2x - (2 - 2x + 2\delta x)y \quad (19)$$

$$\frac{\partial U_E(x,y)}{\partial y} = (\delta - 1)x^2 + 2x - (\delta + C) \quad (20)$$

$$\frac{\partial^2 U_B(x,y)}{\partial x^2} = -2(1-y) - 2\delta y < 0, \quad (21)$$

indicating that $U_B(x,y)$ is concave in x. We consider the following three cases:

1) $\delta = 1$: By (20), we see that $\partial U_E(x,y)/\partial y = 0$ has the unique solution $x_1 = (1 + C)/2$.

1.1) $C > 1$: As $x_1 > 1$, by (20), we have $\partial U_E(x,y)/\partial y < 0$, $\forall\ 0 \le x \le 1$, indicating that $U_E(x,y)$ decreases with y and thus $y^* = 0$. By (19), we have $\partial U_B(x,y^*)/\partial x = 2 - 2x \ge 0$, for $0 \le x \le 1$, and thus $x^* = 1$. The unique NE is $(x^*, y^*) = (1, 0)$.

1.2) $C \le 1$: As $1/2 < x_1 \le 1$, if $x^* = x_1$, $U_E(x^*, y)$ is constant, $\forall\ 0 \le y \le 1$. By (21), $U_B(x,y)$ is concave in x, indicating that the extreme point of $U_B(x,y)$, if exists, is its maximum point. By (19), $\partial U_B(x_1,y)/\partial y = 0$ has $y_1 =$

$(1-C)/2$ and $0 \leq y_1 \leq 1$. Thus, $(x^*, y^*) = (x_1, y_1)$. The uniqueness of the NE is proved as follows:

If $x^* < x_1$, by (20), we have $\partial U_E(x^*, y)/\partial y < 0$, and thus $y^* = 0$. By (19), we have $\partial U_B(x, y^*)/\partial x = 2 - 2x \geq 0$, $\forall\ 0 \leq x \leq 1$ and thus $x^* = 1$. However, as $x^* = 1 \geq x_1$, no NE exists. If $x^* > x_1$, $\partial U_E(x^*, y)/\partial y > 0$, and thus $y^* = 1$. By (19), we have $\partial U_B(x, y^*)/\partial x = -2x \leq 0$, and thus $x^* = 0$, which contradicts with $x^* > x_1$. Thus, (x_1, y_1) is a unique NE.

2) $\delta < 1$: It is clear that $\partial U_E(x, y)/\partial y = 0$ has two solutions denoted by x_2 and $\hat{x}$, respectively, given by

$$x_2 = \frac{-1 - \sqrt{1 + (\delta - 1)(\delta + C)}}{\delta - 1} \tag{22}$$

and

$$\hat{x} = \frac{-1 + \sqrt{1 + (\delta - 1)(\delta + C)}}{\delta - 1}. \tag{23}$$

As $\delta < 1$, we have $x_2 > 1$ and $\hat{x} > 0$.

2.1) $C > 1$: If $1+(\delta-1)(\delta+C) < 0$ or $1+(\delta-1)(\delta+C) \geq 0$ and $\hat{x} > 1$, by (20), we have $\partial U_E(x, y)/\partial y < 0$, $\forall\ 0 \leq x \leq 1$. Similar to Case 1.1, the NE is $(x^*, y^*) = (1, 0)$.

2.2) $C \leq 1$: By (23), we have $\hat{x} \leq 1$. If $x^* = \hat{x}$, $U_E(x^*, y)$ is constant, $\forall\ 0 \leq y \leq 1$. The solution of $\partial U_B(\hat{x}, y)/\partial x = 0$ is given by

$$\hat{y} = \frac{\sqrt{1 + (\delta - 1)(\delta + C)} - \delta}{(1 - \delta)\sqrt{1 + (\delta - 1)(\delta + C)}}, \tag{24}$$

with $0 \leq \hat{y} \leq 1$. By (21), the maximum $U_B(x, \hat{y})$ is achieved at its extreme point, $\hat{x}$. Thus, we have $(x^*, y^*) = (\hat{x}, \hat{y})$. The uniqueness of the NE is shown as follows:

If $x^* < \hat{x}$, by (20), $\partial U_E(x^*, y)/\partial y < 0$ and thus $y^* = 0$. By (19), we have $\partial U_B(x, y^*)/\partial x = 2 - 2x \geq 0$, $\forall\ 0 \leq x \leq 1$ and thus $x^* = 1$, which contradicts with $x^* < \hat{x}$. If $x^* > \hat{x}$, $\partial U_E(x^*, y)/\partial y > 0$, indicating $y^* = 1$. As $U_B(x, y^*) = \delta(1-x^2)+C$, we have $x^* = 0$, which contradicts with $x^* > \hat{x}$. Therefore, $x^* = \hat{x}$.

3) $\delta > 1$: As $C > 0 > 1 + \delta^2/(1 - \delta)$, we have $1 + (\delta - 1)(\delta + C) > 0$. As $\delta > 1$, by (22) and (23), we have $x_2 < 0$ and $\hat{x} > 0$.

3.1) $C > 1$: By (23), we have $\hat{x} > 1$. By (20), $\partial U_E(x, y)/\partial y < 0$, $\forall\ 0 \leq x \leq 1$ and thus $(x^*, y^*) = (1, 0)$, similar to Case 1.1.

3.2) $C \leq 1$: We have $\hat{x} \leq 1$ by (23). If $x^* = \hat{x}$, $U_E(x^*, y)$ is constant, $\forall\ 0 \leq y \leq 1$. It is clear that $\partial U_B(\hat{x}, \hat{y})/\partial x = 0$ by (24). By (21), $U_B(x, y)$ is concave in x, indicating that the maximum $U_B(x, \hat{y})$ is achieved at its extreme point, i.e., $x^* = \hat{x}$. Thus $(x^*, y^*) = (\hat{x}, \hat{y})$. The proof of the uniqueness of this NE is similar to that in Case 2.2. In summary, we have Lemma 1.

REFERENCES

[1] M. C. Domingo, "Securing underwater wireless communication networks," *IEEE Wireless Commun.*, vol. 18, no. 1, pp. 22–28, 2011.

[2] A. Qian, L. Shu, X. Li, G. Han, and J. Rodrigues, "Detecting Sybil attack based on state information in underwater wireless sensor networks," in *Proc. IEEE Int'l Conf. Software, Telecommun. and Computer Networks (SoftCOM)*, pp. 1–5, 2013.

[3] D. Galindo, R. Roman, and J. Lopez, "A killer application for pairings: Authenticated key establishment in underwater wireless sensor networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 5339, pp. 120–132, 2008.

[4] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 56–62, 2010.

[5] W. Trappe and L. Washington, *Introduction to cryptography with coding theory (2nd Edition)*. Prentice Hall, 2005.

[6] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel and Distributed Systems*, vol. 24, no. 1, pp. 44–58, 2013.

[7] F. J. Liu, X. Wang, and S. Primak, "A two dimensional quantization algorithm for CIR-based physical layer authentication," in *Proc. IEEE Int'l Conf. Commun. (ICC)*, pp. 4724–4728, 2013.

[8] L. Xiao, A. Reznik, W. Trappe, and et al., "PHY-authentication protocol for spoofing detection in wireless networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, pp. 6–10, 2010.

[9] H. Liu, Y. Wang, J. Liu, J. Yang, and Y. Chen, "Practical user authentication leveraging channel state information (CSI)," in *Proc. ACM Symp. Inform., Computer and Commun. Security*, pp. 389–400, 2014.

[10] X. Wu and Z. Yang, "Physical-layer authentication for multi-carrier transmission," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 74–77, 2015.

[11] X. Li, G. Han, A. Qian, and et al., "Detecting Sybil attack based on state information in underwater wireless sensor networks," in *Proc. IEEE Int'l Conf. Software, Telecommun. and Computer Networks (SoftCOM)*, pp. 1–5, 2013.

[12] E. Souza, H. Wong, I. Cunha, and et al., "End-to-end authentication in underwater sensor networks," in *Proc. IEEE Symp. Computers and Commun. (ISCC)*, pp. 299–304, 2013.

[13] L. Xiao, Y. Li, G. Liu, Q. Li, and W. Zhuang, "Spoofing detection with reinforcement learning in wireless networks," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, San Diego, CA, 2015.

[14] M. Stojanovic, "On the relationship between capacity and distance in an underwater acoustic communication channel," *ACM SIGMOBILE Mobile Computing and Commun. Review*, vol. 11, no. 4, pp. 34–43, 2007.