Wireless Secret Sharing Game between Two Legitimate Users and an Eavesdropper

Lei Miao, Hongbo Zhang, and Dingde Jiang

Dept. of Engineering Technology, Middle Tennessee State University, Murfreesboro, TN 37132, USA
Dept. of Engineering Technology, Middle Tennessee State University, Murfreesboro, TN 37132, USA
School of Astronautics & Aeronautic, University of Electronic Science and Technology of China, Sichuan, China

Abstract. Wireless secret sharing is crucial to information security in the era of Internet of Things. One method is to utilize the effect of the randomness of the wireless channel in the data link layer to generate the common secret between two legitimate users Alice and Bob. This paper studies this secret sharing mechanism from the perspective of game theory. In particular, we formulate a non-cooperative zero-sum game between the legitimate users and an eavesdropper Eve. In a symmetrical game where Eve has the same probability of successfully receiving a packet from Alice and Bob when the transmission distance is the same, we show that both pure and mixed strategy Nash equilibria exist. In an asymmetric game where Eve has different probabilities of successfully receiving a packet from Alice and Bob, a pure strategy may not exist; in this case, we show how a mixed strategy Nash equilibrium can be found.

Keywords: secret sharing, wireless communications, game theory, Nash equilibrium.

1 Introduction

Security and privacy in wireless networking relies on symmetric-key cryptography, which requires pre-established private keys at both the transmitter and the receiver. In the era of Internet of Things (IoT) where Machine to Machine (M2M) communications frequently occur with minimum human intervention, automatic and secure sharing of secrets for the purpose of cryptography is crucial to information security. There are various ways to share secrets automatically in wireless networks. One direction is to combine cryptographic schemes and channel coding techniques so that transmitted messages between two legitimate users Alice and Bob cannot be decoded by the eavesdropper Eve [1] [2]. Recent works along this line can be found in [3], [4], and [5] for interference, broadcast, and multiple access channels, respectively. Another approach exploits the principle of reciprocity [6] in wireless communications and extracts the secret from the common observation between Alice and Bob on the wireless channel state [7] [8] [9]. All these methods mentioned above are collectively known as the physical layer solutions, which essentially exploit the

David C. Wyld et al. (Eds): AIFZ, SIGPRO, NWCOM, CLSB, MLNLP, DTMN, BDIOT, CSITY - 2022
pp. 29-39, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.121603

randomness and varying nature of wireless channels to share secrets. They do not work very well when the speed of variation in wireless channels is slow and may also require costly modifications to existing communication protocols and infrastructure.

In a different direction, the effect of wireless channel dynamics on the data link layer is utilized to share secrets [10], [11], [12]. The idea behind works along this line is as follows: Alice and Bob keep sending each other unicast packets without retry, using which the secret is derived; Eve would eventually lose a packet and be unable to figure out the secret even if she knew exactly the mechanism Alice and Bob use. More details of this approach can be found in our previous work [13] where we discuss optimal secret sharing between Alice and Bob with the presence of Eve. Specifically, we assume in [13] that Eve's location is random, and only Alice and Bob can choose how to generate the secret; we show that when the probability of successfully transmitting a packet is monotonically decreasing with the transmission distance and Eve's location is uniformly distributed, the optimal strategy for Alice and Bob to minimize the probability that Eve figures out the secret is to generate half of the secret from each one of them.

In this paper, we consider the case that Eve can also choose her location in order to maximize her probability of receiving all packets and figuring out the secret. Specifically, we assume that both the legitimate users (Alice and Bob) and the eavesdropper (Eve) do not know each other's strategy but are both rational. Let P_e be the probability of Eve figuring out the secret. Then, Alice and Bob's goal is to minimize P_e or maximize $-P_e$, and Eve's goal is to maximize P_e. This observation motivates us to formulate the problem as a zero-sum game between the legitimate users and the eavesdropper.

Security games have been studied extensively on the interaction between legitimate and malicious users, and game-theoretic approaches have been applied to a wide range of problems, including security at the physical and MAC layers, security at the application layer, cryptography, etc. For comprehensive reviews, see [14] [15] [16]. Our secret sharing game is different from the existing ones in the literature: we study how to share secrets using the effect of the unreliable nature of wireless channels on the data link layer. Our results are based on the probability function of Eve successfully receiving a packet. Nonetheless, our analysis does not rely on a specific form of the probability function; instead, our work would be applicable to any probability function as long as a mild assumption is satisfied. The main contributions of this paper is as follows: *(i)* We show that the optimal secret sharing problem can be considered as a game between two legitimate users and the eavesdropper; *(ii)* We analyze the symmetric game case and identify both pure and mixed strategy Nash equilibria; *(iii)* For the asymmetric game case, we discover two different scenarios that yield pure and mixed Nash equilibrium, respectively; and *(iv)* We show how the mixed strategy Nash equilibrium can be found when the probabilities of successful packet transmission are known.

The organization of the rest of the paper is as follows: in Section 2, we discuss the system model and formulate the game; in Section 3, we present the main results of the optimal secret sharing zero-sum game; and finally, we conclude in Section 4.

2 System Model and Problem Formulation

In our system model, the two legitimate users Alice and Bob are at two different locations that are D meters away, and they are trying to exchange N packets $\{Pkt_1, Pkt_2, \ldots, Pkt_N\}$, using which the secret is calculated. One simply way to obtain the secret is to exclusive-OR all N packets together: $secret = Pkt_1 \oplus Pkt_2 \oplus \cdots \oplus Pkt_N$. Due to the unreliable nature of wireless communications, Eve will have high probability of losing one or more packets when N is large so that she will not be able to figure out the secret. Without loss of generality, we let N be an even number. For ease of notation, We assume that each of the two game players, i.e., the legitimate users and the eavesdropper, has three strategies. For Alice and Bob, the three strategies are: Alice sends all N packets to Bob, Bob sends all N packets to Alice, and each one of them sends $N/2$ packets to the other. We use S_A, S_B, and S_{AB} to denote these three strategies, respectively. Eve chooses to stay somewhere between Alice and Bob, and she also has three different strategies: stay close to Alice, stay close to Bob, and stay in the exact middle. We use L_A, L_B, and L_M to denote these three locations/strategies, respectively. Note that although we only have three strategies defined for each player, our results can be extended to the cases that more strategies are available. We further assume that locations L_A and L_B are ϵ, $\epsilon \in (0, \frac{D}{2})$, meters away from Alice and Bob, respectively; location L_M is $\frac{D}{2}$ meters away from both Alice and Bob. Thus, $P_A(\epsilon)$, $P_A(D-\epsilon)$, and $P_A(\frac{D}{2})$ are the probabilities of Eve successfully receiving a packet from Alice when Eve's strategy is L_A, L_B, and L_M, respectively. Similarly, $P_B(\epsilon)$, $P_B(D-\epsilon)$, $P_B(\frac{D}{2})$ are the probabilities of Eve successfully receiving a packet from Bob when Eve's strategy is L_B, L_A, and L_M, respectively.

Let $P_A(d)$ and $P_B(d)$ be the probability of Eve successfully receiving a packet from Alice or Bob, respectively, when the transmission distance is d. We have the following assumption about $P_A(d)$ and $P_B(d)$.

(i) Each packet transmission is independent from each other; *(ii)* $P_A(d)$ and $P_B(d)$ are time-invariant; *(iii)* $P_A(\epsilon) > P_A(\frac{D}{2}) > P_A(D-\epsilon)$ and $P_B(\epsilon) > P_B(\frac{D}{2}) > P_B(D-\epsilon)$; and *(iv)* $P_A(\frac{D}{2}) > \frac{1}{2}[P_A(D-\epsilon) + P_A(\epsilon)]$ and $P_B(\frac{D}{2}) > \frac{1}{2}[P_B(D-\epsilon) + P_B(\epsilon)]$. The assumptions above is quite generic and does not require the exact form of functions $P_A(d)$ and $P_B(d)$. Parts *(i)* and *(ii)* above are valid in slow-fading environments where the coherence time of the wireless channel is long and the channel state is stable during the period of secret sharing. Part *(iii)* states that the key factor that determines the probability of successful packet transmission is the distance, which is especially true in long-distance wireless communications. An example of $P_A(d)$ and $P_B(d)$ supporting the monotonicity assumption in VANET

(Vehicular Ad Hoc Networks) environments can be found in [17], in which Killat et al. simulate and verify a theoretical probability of successful transmission function of distance inferred from the Nakagami-m distribution of RF wave propagation. It is well known that in free space, the path loss of RF signals is proportional to the square of distance; part *(iv)* above reflects this: in spite of random factors such as channel fading, the signal's power and the probability of successful transmission attenuates faster when the distance is larger.

3 Optimal Secret Sharing as a Zero-Sum Game

Let s_L and s_E be the strategies of the legitimate users, i.e., Alice and Bob, and Eve, the eavesdropper, respectively. We have $s_L \in \{S_A, S_B, S_{AB}\}$ and $s_E \in \{L_A, L_B, L_M\}$ We use $U_L(s_L, s_E) = -P_e$ and $U_E(s_L, s_E) = P_e$ to denote the utility functions of the legitimate users and Eve, respectively. Essentially, Alice and Bob would like to minimize the probability of Eve figuring out the secret, and Eve would like to maximize the same probability.

Definition 1. *A strategy profile (s_L^*, s_E^*) is a Nash equilibrium if $U_L(s_L^*, s_E^*) \geq U_L(s_L, s_E^*)$ for each feasible strategy s_L and $U_E(s_L^*, s_E^*) \geq U_E(s_L^*, s_E)$ for each feasible strategy s_E.*

3.1 Symmetric Game

We first consider a symmetric game scenario that the following hold:

$$P_A(L_A) = P_B(L_B) = P(\epsilon),\ P_A(L_B) = P_B(L_A) = P(D-\epsilon),$$
$$\text{and } P_A(L_M) = P_B(L_M) = P(D/2).$$

We have the utility matrix shown in Table 1 where the utility functions of Eve are positive and the ones of Alice and Bob are negative. Next, let us first introduce an auxiliary lemma.

Table 1. Utility matrix of the symmeric game.

		Alice and Bob		
		S_A, q_1	S_{AB}, q_2	$S_B, 1-q_1-q_2$
Eve	L_A, p_1	$\pm P^N(\epsilon)$	$\pm P^{\frac{N}{2}}(\epsilon)P^{\frac{N}{2}}(D-\epsilon)$	$\pm P^N(D-\epsilon)$
	L_M, p_2	$\pm P^N(\frac{D}{2})$	$\pm P^N(\frac{D}{2})$	$\pm P^N(\frac{D}{2})$
	$L_B, 1-p_1-p_2$	$\pm P^N(D-\epsilon)$	$\pm P^{\frac{N}{2}}(\epsilon)P^{\frac{N}{2}}(D-\epsilon)$	$\pm P^N(\epsilon)$

Lemma 1. $P^{\frac{N}{2}}(\epsilon)P^{\frac{N}{2}}(D-\epsilon) < P^N(\frac{D}{2})$

Proof: Because $P(\epsilon) \in (0,1)$, $P(D-\epsilon) \in (0,1)$, and $P(\frac{D}{2}) \in (0,1)$, we only need to show that $P(\epsilon)P(D-\epsilon) < P^2(\frac{D}{2})$. Because $\epsilon \in (0, \frac{D}{2})$, $D-\epsilon \neq \epsilon$. Since $P(\cdot)$ is monotonically decreasing, we have

$$[P(D-\epsilon) - P(\epsilon)]^2 = P^2(D-\epsilon) + P^2(\epsilon) - 2P(D-\epsilon)P(\epsilon) > 0,$$

i.e.,

$$\frac{1}{4}[P^2(D-\epsilon) + P^2(\epsilon)] > \frac{1}{2}[P(D-\epsilon)P(\epsilon)]. \tag{1}$$

From part *(iv)* of Assumption 2, we have

$$\begin{aligned} P^2(\frac{D}{2}) &= P^2(\frac{1}{2}(D-\epsilon) + \frac{1}{2}\epsilon) > [\frac{1}{2}P(D-\epsilon) + \frac{1}{2}P(\epsilon)]^2 \\ &= \frac{1}{4}[P^2(D-\epsilon) + P^2(\epsilon)] + \frac{1}{2}[P(D-\epsilon)P(\epsilon)] \end{aligned}$$

Invoking (1), we have $P^2(\frac{D}{2}) > P(D-\epsilon)P(\epsilon)$ ■.

We are now ready to discuss the pure strategy result of the symmetric game.

Lemma 2. *Strategy profile (S_{AB}, L_M) is a pure strategy Nash equilibrium.*

Proof: It can be seen from the utility matrix that $U_L(S_{AB}, L_M) = U_L(S_A, L_M) = U_L(S_B, L_M) = -P^N(\frac{D}{2})$. Invoking Lemma 1, we have

$$U_E(S_{AB}, L_M) = P^N(\frac{D}{2}) > P^{\frac{N}{2}}(\epsilon)P^{\frac{N}{2}}(D-\epsilon) = U_E(S_{AB}, L_A) = U_E(S_{AB}, L_B).$$

From Definition 1, it follows that strategy profile (S_{AB}, L_M) is a pure strategy Nash equilibrium. ■

Lemma 2 indicates that in the pure strategy Nash equilibrium, Alice and Bob each generates half of the packets and Eve stays in the middle location L_M. We now turn our attention to a mixed strategy Nash equilibrium, in which Eve has probabilities p_1, p_2, and $p_3 = 1 - p_1 - p_2$ to use strategies L_A, L_M, and L_B, respectively; similarly, Alice and Bob have probabilities q_1, q_2, and $q_3 = 1 - q_1 - q_2$ to use strategies S_A, S_{AB}, and S_B, respectively.

Lemma 3. *In a mixed strategy Nash equilibrium, Eve's strategy is to stay at L_M with probability 1; Alice and Bob should have positive probabilities on all three strategies S_A, S_B, and S_{AB} so that:*

$$q_1P^N(\epsilon) + q_2P^{\frac{N}{2}}(\epsilon)P^{\frac{N}{2}}(D-\epsilon) + q_3P^N(D-\epsilon) < P^N(\frac{D}{2}) \tag{2}$$

and

$$q_1P^N(D-\epsilon) + q_2P^{\frac{N}{2}}(D-\epsilon)P^{\frac{N}{2}}(\epsilon) + q_3P^N(\epsilon) < P^N(\frac{D}{2}) \tag{3}$$

Proof: Suppose that $0 < q_1 < 1$, $0 < q_2 < 1$, and $0 < 1 - q_1 - q_2 < 1$. In a mixed strategy Nash equilibrium, we have:

$$\begin{aligned}
&- p_1 P^N(\epsilon) - p_2 P^N(\frac{D}{2}) - (1 - p_1 - p_2) P^N(D - \epsilon) \\
&= -p_1 P^{\frac{N}{2}}(\epsilon) P^{\frac{N}{2}}(D - \epsilon) - p_2 P^N(\frac{D}{2}) - (1 - p_1 - p_2) P^{\frac{N}{2}}(\epsilon) P^{\frac{N}{2}}(D - \epsilon) \\
&= -p_1 P^N(D - \epsilon) - p_2 P^N(\frac{D}{2}) - (1 - p_1 - p_2) P^N(\epsilon)
\end{aligned}$$

Solving the above equations, we get $p_1 = p_3 = 0$, and $p_2 = 1$. If it is the case in the mixed strategy Nash equilibrium, we must also have (2) and (3).

Next, we verify that when (2) and (3) hold, $\exists\ q_1, q_2$, and q_3 so that $0 < q_1 < 1$, $0 < q_2 < 1$, and $0 < q_3 < 1$. Let $q_1 = q_3$, and (2) and (3) become one inequality:

$$2q_1[P^N(\epsilon) + P^N(D - \epsilon)] + q_2 P^{\frac{N}{2}}(\epsilon) P^{\frac{N}{2}}(D - \epsilon) < P^N(\frac{D}{2}) = 2q_1 P^N(\frac{D}{2}) + q_2 P^N(\frac{D}{2}) \tag{4}$$

Invoking Lemma 1, we have $q_2 P^{\frac{N}{2}}(\epsilon) P^{\frac{N}{2}}(D - \epsilon) < q_2 P^N(\frac{D}{2})$. We now consider two cases.

Case 1: $2q_1[P^N(\epsilon) + P^N(D - \epsilon)] \leq 2q_1 P^N(\frac{D}{2})$. In this case, (4) always holds as long as q_1, q_2, and q_3 are nonzero probabilities.

Case 2: $2q_1[P^N(\epsilon) + P^N(D - \epsilon)] > 2q_1 P^N(\frac{D}{2})$. In this case, we can always pick small enough positive q_1 and q_3 values so that (4) holds. ■

3.2 Asymmetric Game

We now consider an asymmetric game scenario that $P_A(d) > P_B(d)$, i.e., when the transmission distance is the same, Eve has higher probability to successfully receive a packet from Alice than from Bob. For example, if Alice has higher transmission power than Bob or Bob is closer to a noise source, then the signal to noise ratio between Alice and Eve may be higher than that between Bob and Eve, causing the asymmetric game scenario described above. We have the following utility matrix shown in Table 2.

Table 2. Utility matrix of the asymmeric game.

		Alice and Bob		
		S_A, q_1	S_{AB}, q_2	$S_B, 1 - q_1 - q_2$
Eve	L_A, p_1	$\pm P_A^N(\epsilon)$	$\pm P_A^{\frac{N}{2}}(\epsilon) P_B^{\frac{N}{2}}(D - \epsilon)$	$\pm P_B^N(D - \epsilon)$
	L_M, p_2	$\pm P_A^N(\frac{D}{2})$	$\pm P_A^{\frac{N}{2}}(\frac{D}{2}) P_B^{\frac{N}{2}}(\frac{D}{2})$	$\pm P_B^N(\frac{D}{2})$
	$L_B, 1 - p_1 - p_2$	$\pm P_A^N(D - \epsilon)$	$\pm P_B^{\frac{N}{2}}(\epsilon) P_A^{\frac{N}{2}}(D - \epsilon)$	$\pm P_B^N(\epsilon)$

Note that similar to the utility matrix in the symmetric game case, we only show the utility functions of Eve; the ones of Alice and Bob are negative and are not shown above.

Lemma 4. *If $P_A(d) > P_B(d)$, and $P_B(\epsilon) \leq P_A(D-\epsilon)$, then strategy profile (S_B, L_B) is a pure strategy Nash equilibrium.*

Proof: Because $\epsilon \in (0, D/2)$ and $P_B(d)$ is monotonically decreasing, we have

$$P_B^N(\epsilon) > P_B^N(\frac{D}{2}) > P_B^N(D-\epsilon), \text{i.e.,}$$

$$U_E(S_B, L_B) > U_E(S_B, L_M) > U_E(S_B, L_A). \tag{5}$$

By assumption, $P_B(\epsilon) \leq P_A(D-\epsilon)$, we get

$$P_B^N(\epsilon) \leq P_B^{\frac{N}{2}}(\epsilon) P_A^{\frac{N}{2}}(D-\epsilon) \leq P_A^N(D-\epsilon). \tag{6}$$

Multiplying (6) by -1 yields:

$$-P_B^N(\epsilon) \geq -P_B^{\frac{N}{2}}(\epsilon) P_A^{\frac{N}{2}}(D-\epsilon) \geq -P_A^N(D-\epsilon), \text{i.e.,}$$

$$U_L(S_B, L_B) \geq U_L(S_{AB}, L_B) \geq U_L(S_A, L_B). \tag{7}$$

Combining (5) and (7), it follows that strategy profile (S_B, L_B) is a pure strategy Nash equilibrium. ■

The intuition behind Lemma 4 is that if $P_B(d)$ is so much less than $P_A(d)$ so that $P_B(\epsilon) \leq P_A(D-\epsilon)$, then the best strategy of the legitimate users is to always let Bob send the packets; conversely, the best strategy of Eve is to stay close to Bob so that she could maximize the probability of receiving all packets.

Lemma 5. *If $P_A(d) > P_B(d)$ and $P_B(\epsilon) > P_A(D-\epsilon)$, then there is no pure strategy Nash equilibrium.*

Proof: We discuss the three columns of the utility matrix individually.
(1) Column #1: We have $U_E(S_A, L_A) = P_A^N(\epsilon) > U_E(S_A, L_M) = P_A^N(\frac{D}{2}) > U_E(S_A, L_B) = P_A^N(D-\epsilon)$ due to part *(iii)* of Assumption 2. Therefore, only strategy profile (S_A, L_A) can possibly be a pure strategy in the first column. However, we have $U_L(S_A, L_A) = -P_A^N(\epsilon) < -P_B^N(\epsilon) < -P_B^N(D-\epsilon) = U_L(S_B, L_A)$ in the first row. Therefore, there is no pure strategy Nash equilibrium in the first column of the utility matrix.
(2) Column #2: Because $U_E(S_A, L_A) = P_A^N(\epsilon) > U_E(S_{AB}, L_A) = P_A^{\frac{N}{2}}(\epsilon) P_B^{\frac{N}{2}}(D-\epsilon) > U_E(S_B, L_A) = P_B^N(D-\epsilon)$, strategy profile (S_{AB}, L_A) cannot be a pure strategy Nash equilibrium. Similarly, because $U_E(S_A, L_M) = P_A^N(\frac{D}{2}) > U_E(S_{AB}, L_M) = P_A^{\frac{N}{2}}(\frac{D}{2}) P_B^{\frac{N}{2}}(\frac{D}{2}) > U_E(S_B, L_M) = P_B^N(\frac{D}{2})$, strategy profile (S_{AB}, L_M) cannot be

a pure strategy Nash equilibrium either. Finally, because $U_E(S_A, L_B) = P_A^N(D - \epsilon) < U_E(S_{AB}, L_B) = P_A^{\frac{N}{2}}(D - \epsilon)P_B^{\frac{N}{2}}(\epsilon) < U_E(S_B, L_B) = P_B^N(\epsilon)$, strategy profile (S_{AB}, L_B) cannot be a pure strategy Nash equilibrium.
(3) Column #3: Similarly to the Column #1 case, there is no pure strategy Nash equilibrium in the third column either. The analysis is very similar to the Column #1 case, and we omit the details. ■

Lemma 5 shows that when $P_B(\epsilon) > P_A(D - \epsilon)$, i.e., $P_B(d)$ is not too much less than $P_A(d)$, no pure strategy Nash equilibrium exists. According to [18], at least one mixed strategy Nash equilibrium always exists in this case. The utility functions are:

$$-p_1 P_A^N(\epsilon) - p_2 P_A^N(\frac{D}{2}) - p_3 P_A^N(D - \epsilon) \quad (q_1)$$

$$-p_1 P_A^{\frac{N}{2}}(\epsilon) P_B^{\frac{N}{2}}(D - \epsilon) - p_2 P_A^{\frac{N}{2}}(\frac{D}{2}) P_B^{\frac{N}{2}}(\frac{D}{2}) - p_3 P_B^{\frac{N}{2}}(\epsilon) P_A^{\frac{N}{2}}(D - \epsilon) \quad (q_2)$$

$$-p_1 P_B^N(D - \epsilon) - p_2 P_B^N(\frac{D}{2}) - p_3 P_B^N(\epsilon \quad (q_3)$$

$$q_1 P_A^N(\epsilon) + q_2 P_A^{\frac{N}{2}}(\epsilon) P_B^{\frac{N}{2}}(D - \epsilon) + q_3 P_B^N(D - \epsilon) \quad (p_1)$$

$$q_1 P_A^N(\frac{D}{2}) + q_2 P_A^{\frac{N}{2}}(\frac{D}{2}) P_B^{\frac{N}{2}}(\frac{D}{2}) + q_3 P_B^N(\frac{D}{2}) \quad (p_2)$$

$$q_1 P_A^N(D - \epsilon) + q_2 P_B^{\frac{N}{2}}(\epsilon) P_A^{\frac{N}{2}}(D - \epsilon) + q_3 P_B^N(\epsilon) \quad (p_3)$$

where (q_1), (q_2), and (q_3) are the payoffs of the legitimate users when strategies S_A, S_{AB}, and S_B are used, respectively; (p_1), (p_2), and (p_3) are the payoffs of Eve when strategies L_A, L_M, and L_B are used, respectively. The procedure of finding the mixed strategy Nash equilibrium involves two steps: *proposition* and *verification*. In the first step, we make an assumption about either $\{p_1, p_2, p_3\}$ or $\{q_1, q_2, q_3\}$ and use the utilization functions to solve for the other set of probabilities. If the solution is feasible and we are able to use it in the second step to verify that the proposition provided in Step 1 is indeed true, the Nash equilibrium is found. Next, we formally present the procedure in Algorithm 1 where we only show the propositions about $\{p_1, p_2, p_3\}$; the pseudo code of making propositions about $\{q_1, q_2, q_3\}$ is very similar.

3.3 Numerical Example

In this subsection, we present a numerical example. For ease of calculation, we let $N = 2$. The probabilities are: $P_A(\epsilon) = 0.99$, $P_A(\frac{D}{2}) = 0.94$, $P_A(D - \epsilon) = 0.80$, $P_B(\epsilon) = 0.90$, $P_B(\frac{D}{2}) = 0.84$, and $P_B(D - \epsilon) = 0.70$. Invoking Lemma 5, there is no pure strategy Nash equilibrium. The mixed strategy utility functions corresponding to (q_1) through (p_3) are:

$$-0.3401p_1 - 0.2364p_2 - 0.64 \quad (8)$$

Algorithm 1 Finding mixed strategy Nash equilibrium in an asymmetric game when $P_B(\epsilon) > P_A(D-\epsilon)$

Proposition: enumerate the following assumptions.
p_1, p_2, and p_3 are all non-zero probabilities; solve (p_1)=(p_2)=(p_3) for q_1, q_2, q_3 and go to Verification.
For any two probabilities p' and p'' $\in\{p_1, p_2, p_3\}$, assume they are non-zero and use p''' to denote the remaining probability. Solve (p')=(p'')>(p''') for q_1, q_2, q_3 and go to Verification.
Verification:
if the solution is infeasible **then**
    Continue to the next assumption
else
    if q_1,q_2, and q_3 are all positive **then**
        Solve (q_1)=(q_2)=(q_3) for p_1, p_2, p_3.
    end if
    if two probabilities q' and q'' $\in\{q_1, q_2, q_3\}$ are positive, and the remaining probability q''' is 0 **then**
        Solve $(q') = (q'') > (q''')$ for p_1, p_2, p_3.
    end if
    if q' $\in\{q_1, q_2, q_3\}$ is 1, and the other two probability q'' and q''' are 0 **then**
        Solve $(q') > (q'')$ and $(q') > (q''')$ for p_1, p_2, p_3.
    end if
    if the solution of p_1, p_2, p_3 matches with the proposition **then**
        Nash equilibrium is found and exit
    else
        Continue to the next assumption
    end if
end if

$$0.027p_1 - 0.0504p_2 - 0.72 \tag{9}$$

$$0.32p_1 + 0.1044p_2 - 0.81 \tag{10}$$

$$0.4901q_1 + 0.203q_2 + 0.49 \tag{11}$$

$$0.178q_1 + 0.084q_2 + 0.7056 \tag{12}$$

$$-0.17q_1 - 0.09q_2 + 0.81 \tag{13}$$

We start out by assuming that $p_1 \in (0,1)$, $p_2 \in (0,1)$, and $1 - p_1 - p_2 \in (0,1)$. Under this proposition, we have (11) = (12) = (13), whose solution is $q_1 = 1.946$, $q_2 = -3.292$, and $1 - q_1 - q_2 = 2.346$. This is infeasible, meaning that p_1, p_2, and $1 - p_1 - p_2$ cannot be all positive and less than 1.

Next, we discuss three cases of p_1, p_2, and $1 - p_1 - p_2$.

Case 1: $p_1 \in (0,1)$, $p_2 \in (0,1)$, and $1-p_1-p_2 = 0$. It yields that (11) = (12) > (13). There are two solutions that ensure q_1, q_2, and $1 - q_1 - q_2$ are not all positive and less than 1. Therefore, we have two subcases:

Case 1.1: $q_1 = 0.6908$, $q_2 = 0$, and $1-q_1-q_2 = 0.3092$. It implies that at equilibrium, we must have (8) = (10) > (9), which has no solution between 0 and 1 for p_1 and p_2.

Case 1.2: $q_1 = 0.5469$, $q_2 = 0.4531$, and $1-q_1-q_2 = 0$. It implies that at equilibrium, we must have (8) = (9) > (10), which has solutions of p_1 and p_2 so that $p_1 + p_2 \in (0,1)$. It implies that $1 - p_1 - p_2 \in (0,1)$, which is impossible.

Case 2: $p_1 \in (0,1)$, $p_2 = 0$, and $1-p_1-p_2 \in (0,1)$. It yields that (11) = (13) > (12). There are no solutions.

Case 3: $p_1 = 0$, $p_2 \in (0,1)$, and $1 - p_1 - p_2 \in (0,1)$. In this last case, we have (12) = (13) > (11). The only feasible solution to it is $q_1 = 0$, $q_2 = 0.6$, and $1 - q_1 - q_2 = 0.4$. If this solution is also the one in equilibrium, we need to have (9) = (10) > (8), which also has a feasible solution: $p_1 = 0$, $p_2 = 0.5814$, and $1 - p_1 - p_2 = 0.4186$.

It completes the numerical example, and the mixed Nash equilibrium is as follows:

$$(p_1, p_2, 1 - p_1 - p_2) = (0, 0.5814, 0.4186)$$
$$(q_1, q_2, 1 - q_1 - q_2) = (0, 0.6, 0.4)$$

4 Conclusions

We have studied the optimal secret sharing problem between two legitimate users (Alice and Bob) and an eavesdropper (Eve), formulated as a non-cooperative zero-sum game. In the symmetric game case, both pure and mixed strategy Nash equilibria exist. Our results indicate that regardless of the type of the equilibrium, Eve should always stay in the middle of Alice and Bob. In the pure strategy Nash equilibrium, the best strategy of Alice and Bob is to generate half of the packets from each

one of them; in a mixed strategy Nash equilibrium, Alice and Bob could generate all the packets from one user only, but some inequalities involving the probabilities must hold.

In the asymmetric game case that Eve has better chance to successfully receive packets from Alice than from Bob, we show that there are two scenarios: if it is very asymmetrical, then a pure strategy Nash equilibrium exists, in which Bob is the one who generates all the packets and Eve chooses to stay near Bob; o.w., a mixed strategy equilibrium exists and can be calculated.

References

1. Barros J, Rodrigues MRD. Secrecy Capacity of Wireless Channels. In: ; 2006; Seattle, WA.
2. Maurer UM. Secret Key Agreement by Public Discussion from Common Information. *IEEE Trans. on Information Theory* 1993; 39: 733-742.
3. Chen J. Secure communication over interference channel: To jam or not to jam?. *IEEE Transactions on Information Theory* 2019; 66(5): 2819–2841.
4. Hyadi A, Rezki Z, Alouini MS. Securing Multi-User Broadcast Wiretap Channels with Finite CSI Feedback. *IEEE Transactions on Information Theory* 2020.
5. Mukherjee P, Ulukus S. Secure degrees of freedom of the multiple access wiretap channel with multiple antennas. *IEEE Transactions on Information Theory* 2018; 64(3): 2093–2103.
6. Balanis CA. *Antenna Theory: Analysis and Design*. New York: John Wiley and Sons. 2nd ed. 1997.
7. Mathur S, Trappe W, Mandayam N, Ye C, Reznik A. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In: ; 2008; San Francisco, CA, USA.
8. Miao L. Differential Secret Sharing in Wireless Networks. *IEEE Wireless Communications Letters* 2015; 4(2): 213-216.
9. Ruotsalainen H, Zhang J, Grebeniuk S. Experimental Investigation on Wireless Key Generation for Low-Power Wide-Area Networks. *IEEE Internet of Things Journal* 2019; 7(3): 1745–1755.
10. Xiao S, Gong W, Towsley D. Secure Wireless Communication with Dynamic Secrets. In: ; 2010; San Diego, CA.
11. Yao T, Fukui K, Nakashima J, Nakai T. Initial common secret key sharing using random plaintexts for short-range wireless communications. *IEEE Trans. on Consumer Electronics* 2009; 55: 2025-2033.
12. Safaka I, Fragouli C, Argyraki K, Diggavi S. Creating shared secrets out of thin air. In: ACM. ; 2012: 73–78.
13. Miao L, Jiang D. Optimal secret sharing for wireless information security in the era of Internet of Things. *Personal and Ubiquitous Computing* 2019: 1–16.
14. Manshaei MH, Zhu Q, Alpcan T, Bacşar T, Hubaux JP. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR)* 2013; 45(3): 1–39.
15. Abdalzaher MS, Seddik K, Elsabrouty M, Muta O, Furukawa H, Abdel-Rahman A. Game theory meets wireless sensor networks security requirements and threats mitigation: A survey. *Sensors* 2016; 16(7): 1003.
16. Do CT, Tran NH, Hong C, et al. Game theory for cyber security and privacy. *ACM Computing Surveys (CSUR)* 2017; 50(2): 1–37.
17. Killat M, Hartenstein H. An empirical model for probability of packet reception in vehicular ad hoc networks. *EURASIP Journal on Wireless Communications and Networking* 2009; 2009(721301): 12.
18. Nash J. Non-cooperative games. *Annals of mathematics* 1951: 286–295.