Cooperative Interference Based on Evolutionary Game in Wire-Tap Channel

Kaizhi Huang, Ying Hong, Wenyu Luo, and Shengbin Lin

Abstract—In wireless network, when using classical game theory to study physical layer security, the energy-limited transmission nodes tend to choose non-cooperative strategy in order to maximize their own secrecy rate, resulting in reduced network secrecy rate. To solve this problem, the paper proposes a cooperative interference method for physical layer security based on evolutionary game. First, it defines the strategies (sending artificial noise or signal) and benefits (secrecy rate under different strategy combination) according to the evolutionary game. Then, the transmission nodes adjust strategy to maximize benefits based on current network state and difference between cooperation benefit and average expected benefit; Finally, the conditions that the transmitting nodes can cooperate with each other could achieve, and the network is evolution from an unstable state to a stable cooperative state to improve the secrecy rate of the system. Simulation and analysis results show that under the Gaussian channel, compared to the traditional game method, the network secrecy rate of the proposed method can be improved 1bit/s/Hz.

Index Terms—Secrecy rate, evolutionary game, cooperative interference, eavesdropper.

I. INTRODUCTION

Wireless networks are vulnerable to be eavesdropped, interfered and attacked for its broadcast features, which always cause a series of security issues. To solve these threats, it is of great importance to adopt an appropriate security mechanism, which can provide confidentiality, integrity and availability. Key management is an important cornerstone of building a secure wireless network and achieving varieties of upper security application in traditional encryption methods. However, the changes in the network topology pose huge challenges to transport and distribute keys. User keys update frequently so that the current encryption algorithms exist with high complexity. In recent years, the new proposed transmission physical layer security methods are based on wire-tap channel model, combining the use of channel coding, amplify and forward, and cooperation. These methods can greatly enhance the safety performance of the whole network without increasing the network load [1]-[3].

In recent years, researches based on game theory for improving network security in physical layer have been widely concerned. Game theory provides a general mathematical framework for studying the interaction between nodes. Zhang Rong-qing proposed a distributed-buyers /sellers game theory framework, which is based on the cooperation in multi-transmitter for wireless cooperative networks [4] in 2012. The secrecy rate can be obviously improved by the interference signals, which is sent by the friendly interference relays. In 2013, Zhou Jie studied a network with four transmitters, including two transmitters, a two-way relay and a jammer [3] in game theory. The optimal equilibrium point is achieved by Stackelberg model. Yet, the existing researches based on classical game theory just offer the strategies to maximize the secrecy rate of a single transmitter, ignoring the secrecy rate of the entire network. The secrecy rate of network depends on the transmitter, which has the lowest secrecy rate in battlefield wireless communication, multi-hop wireless communication [6] and other scenes.

To solve this problem, this paper proposes a cooperative method based on evolutionary game theory in physical layer. Firstly, we build a networking model consisting of two transmitters. One of them sends signals, while the other sends artificial noise to interfere eavesdroppers. Afterwards, we define the strategy and the secrecy rate benefits of different combinations of strategies using evolutionary game mechanisms [7]-[9]. At the same time, we describe the strategy dynamic update process by the replicator dynamics equation. According to the difference between the average expected benefits and that under the current network status and the cooperative strategy, the transmitter continuously adjusts strategies to maximize their benefits. The transmitter learns strategies with a higher secrecy rate and eliminates ineffective strategies in constant process of repeated game. Finally, we obtain the conditions of stable cooperative strategies in transmitter by calculations. In such conditions, the network is evolution from an unstable state to a stable cooperative state with the secrecy rate of the system increasing. Simulation and analysis results show that under the Gaussian channel, the network security rate of the proposed method is 1bit/s/Hz more than that of the classical game theory, when the transmit power meet the conditions of stable cooperative strategies.

II. NETWORK MODELING AND QUESTIONS

A. Network Modeling

The wireless network model with an eavesdropper is shown in Fig. 1, including many transmitters, a receiver and
In a classic game, each player is assumed entirely rational, that is a transmitter can correctly choose strictly dominant strategy to maximize its security rate. For $T_i$, if $T_i$ chooses no cooperation, because $R_i(y, r) > R_i(x, r)$, so $T_i$ chooses no cooperation to get a higher security rate. If $T_j$ chooses cooperation, $T_i$ also chooses no cooperation that to get a high security rate. So, no cooperation is the dominant strategy for $T_i$. Similarly, for $T_j$, it will also choose no cooperation as the dominant strategy. Thus, dominant strategy (no cooperation, no cooperation) is the Nash Equilibrium in a classic game. The transmitter within a bad channel condition, that cannot get cooperation benefit from another transmitter, may be tapped amount of information by eavesdropper.

To solve this problem, this paper proposes a method for security cooperation based on evolutionary game. In Fig. 3, from the player’s perspective, participants of evolutionary game are all of transmitters. When a transmitter finishes a game, it will broadcast its strategies and corresponding benefits to all of other transmitters in networks. Then, from the perspective of the game rules, the transmitter based on the current network status and the difference benefits between cooperation and the mean, adjusting strategy to maximize benefits. Finally, the evolution game is determined by the only stable strategy to achieve a stable equilibrium network. Base on that, this paper proposes a method for physical layer security cooperation to achieve a stable equilibrium (cooperation, cooperation) in a group, thus transmitter in bad channel conditions that cannot get cooperation benefit from another transmitter, may be tapped amount of information by eavesdropper.

To solve this problem, this paper proposes a method for security cooperation based on evolutionary game. In Fig. 3, from the player’s perspective, participants of evolutionary game are all of transmitters. When a transmitter finishes a game, it will broadcast its strategies and corresponding benefits to all of other transmitters in networks. Then, from the perspective of the game rules, the transmitter based on the current network status and the difference benefits between cooperation and the mean, adjusting strategy to maximize benefits. Finally, the evolution game is determined by the only stable strategy to achieve a stable equilibrium network. Base on that, this paper proposes a method for physical layer security cooperation to achieve a stable equilibrium (cooperation, cooperation) in a group, thus transmitter in bad channel conditions that cannot get cooperation benefit from another transmitter, may be tapped amount of information by eavesdropper.

**Fig. 3.** Difference between classic game and evolutionary game.

### III. COOPERATION SECURITY METHOD BASED ON EVOLUTIONARY GAME

First, we introduce the strategy and benefit in evolutionary game. The strategy is to send artificial noise or signal and the benefit is the security rates corresponding to the different strategies. Then, the replicator dynamics equation is used to describe the dynamic update process of the sending strategy, each transmitter adjusts the strategy to maximize benefit according to the current network status and the difference between benefits under the cooperation strategy and average expected. Finally, analyze the condition that the cooperation is the only evolutionary stable strategy, making network evolution from an unstable state to a stable state.

#### A. Strategy Update at the Transmitter

By comparing the wire-tap channel gain, the game participants are divided into two groups. When the wire-tap channel gain meets $h>1$, the transmitter belongs to $M_1$. When the wire-tap channel gain meets $h<1$, the transmitter belongs to $M_2$. The average expected benefit at the transmitter is defined as follows:

**Definition 3.1** average expected benefit: the cooperative ratio in $M_i$ is given as $X$ and the non-cooperative ratio is given as $Y$. While the cooperative ratio in $M_i$ is given as $X$ and the non-cooperative ratio is given as $Y$. Then the average expected benefit is defined as

$$E_{M_i} = X E_{M_i}^C + (1-X) E_{M_i}^N \text{, } (12)$$

$$E_{M_i} = Y E_{M_i}^C + (1-Y) E_{M_i}^N \text{, } (13)$$

where $E_{M_i}^C$, $E_{M_i}^N$ and $E_{M_i}^N$ denote the expected benefit function of cooperative strategy and no cooperative strategy.

The probability of $T_i$ belonging to $M_i$ is $p$ and the probability of $T_i$ belonging to $M_2$ is $q$. Let $q=1-p$ . Then we will get four kinds of networking strategy in $M_i$: ( $M_i$ cooperation, $M_i$ cooperation), ( $M_i$ cooperation, $M_2$ no cooperation), ( $M_2$ cooperation, $M_i$ cooperation), ( $M_2$ cooperation, $M_2$ no cooperation). Finally, we get the average expected benefit of cooperation in $M_i$:

$$E_{M_i}^C = p^i(X R_{i}^C + (1-X) R_{i}^C) _{h \in k \& l} + pq(Y R_{i}^C + (1-Y) R_{i}^C)_{h \in k \& l} \text{, } (14)$$

Similarly, the average expected benefit of no cooperation in $M_i$ is

$$E_{M_i}^N = p^i(X R_{i}^N + (1-X) R_{i}^N) _{h \in k \& l} + pq(Y R_{i}^N + (1-Y) R_{i}^N)_{h \in k \& l} \text{, } (15)$$

The average expected benefit of cooperation in $M_2$ is

$$E_{M_2}^C = q^i(Y R_{i}^C + (1-Y) R_{i}^C) _{h \in k \& l} + pq(Y R_{i}^C + (1-Y) R_{i}^C)_{h \in k \& l} \text{, } (16)$$

The average expected benefit of no cooperation in $M_2$ is

$$E_{M_2}^N = q^i(Y R_{i}^N + (1-Y) R_{i}^N) _{h \in k \& l} + pq(Y R_{i}^N + (1-Y) R_{i}^N)_{h \in k \& l} \text{, } (17)$$

By establishing the replicator dynamics equation, the transmitter constantly adjusts their strategies to maximize the benefits. Using $dx/dt$ indicating the changing proportion rate of participants using cooperative strategy, the replicator dynamics equation in $M_i$ is expressed as

$$dX/dt = X \left[ E_{M_i}^C - E_{M_i} \right] = X \left[ E_{M_i}^C - X E_{M_i}^C - (1-X) E_{M_i}^N \right] \text{, } (18)$$

Formula(18) has two stable states at most, respectively, $x^* = 0$ and $x^* = 1$.

Using $dy/dt$ indicating the changing proportion rate of participants using no cooperative strategy, the replicator dynamics equation in $M_i$ is expressed as

$$dY/dt = Y \left[ E_{M_i}^N - E_{M_i} \right] = Y \left[ E_{M_i}^N - Y E_{M_i}^N - (1-Y) E_{M_i}^C \right] \text{, } (19)$$

Formula(19) has two stable states at most, respectively, $y^* = 0$ and $y^* = 1$.

According to evolutionary game theory, the formula (18) and (19) constitute the inter-relay transmission dynamic replication system. For any initial point.
network is \( \det J > 0 \), \( \text{tr} J < 0 \). By substituting \( (X=1,Y=1) \) into Jacobian \( J \), we will obtain
\[
J = \begin{bmatrix}
E & 0 \\
0 & F 
\end{bmatrix}
\]  
(21)

The determinant of the matrix is
\[
\det J = EF > 0
\]
(22)

The trace of the matrix is
\[
\text{tr} J = E + F < 0
\]
(23)

As \( \text{tr} J = E + F \) is constant less than 0, when \( \det J = EF \) is greater than 0, \( E \) is constant less than 0. Then \( F = pq(R^{r^*})_{h_1\alpha_1\gamma_1} - q^*(R^{r^*})_{h_1\alpha_1\gamma_1} - pq(R^{r^*})_{h_1\alpha_2\gamma_2} < 0 \), we will obtain
\[
p < p^* = \min \left( \frac{(R^{r^*})_{h_1\alpha_1\gamma_1}}{(R^{r^*})_{h_1\alpha_2\gamma_2} + (R^{r^*})_{h_1\alpha_2\gamma_1} - (R^{r^*})_{h_1\alpha_1\gamma_1}} \right)
\]  
(24)

Uniqueness
When \( p < p^* \), \((0,0), (1,0), (0,1)\) are the unstable points and cooperation is the unique evolutionary stable strategy for network. At this time, no cooperative strategy will gradually disappear in the network strategy update process and cooperative strategy become the only evolutionary stable strategy, specifically as shown in Table II.

**TABLE II: STABILITY OF THE NETWORK EQUILIBRIUM POINT**

<table>
<thead>
<tr>
<th>Equilibrium Point(X,Y)</th>
<th>( \det J )</th>
<th>( \text{tr} J )</th>
<th>Stability</th>
</tr>
</thead>
<tbody>
<tr>
<td>((1,1))</td>
<td>&gt;0</td>
<td>+</td>
<td>ESS</td>
</tr>
<tr>
<td>((0,1))</td>
<td>=0</td>
<td>&lt;0</td>
<td>Unstable</td>
</tr>
<tr>
<td>((1,0))</td>
<td>=0</td>
<td>&lt;0</td>
<td>Unstable</td>
</tr>
<tr>
<td>((0,0))</td>
<td>=0</td>
<td>&lt;0</td>
<td>Unstable</td>
</tr>
</tbody>
</table>

Steps of cooperative security based on evolutionary game are as follows:

1) Two nearest transmitters form group and they transmit signals to the legitimate receiver during each half slot.

2) By comparing the wire-tap channel gain, the game participants are divided into two groups: \( M_1 \) and \( M_2 \). The cooperative ratio in \( M_1 \) is \( X \) and the cooperative ratio in \( M_2 \) is \( Y \). The probability of \( T_1 \) belonging to \( M_1 \) is \( p \) and the probability of \( T_1 \) belonging to \( M_2 \) is \( q \).

3) According to the benefits feedback from all individuals, \( M_1 \) and \( M_2 \) obtain the expected benefits \( E^{m_1}_{X} \), \( E^{m_2}_{Y} \) under cooperation and average expected benefits \( E_{X} \), \( E_{Y} \).

4) According to the dynamic equation
\[
dX / dt = X[E^{m_1}_{X} - E_{X}], \quad dY / dt = Y[E^{m_2}_{Y} - E_{Y}], \quad M_1 \text{ and } M_2 \text{ update the proportion } X, Y \text{ of cooperative strategy.}
\]

5) We can get partial equilibrium point of the network by
\[
dX / dt = 0, \quad dY / dt = 0.
\]

6) Through Theorem 3.1, we obtain the condition for cooperation being the only evolutionary stable strategy at the transmitter.
Step 1: The designated recipient \( U_r \) computes
\[
R = C_2 \oplus C_1^{x_r} \mod p, \tag{22}
\]
\[
K = Q \oplus C_1^{x_r} \mod p. \tag{23}
\]

Step 2: The recipient \( U_r \) recovers the message \( M \) by computing
\[
M = R \oplus (g^S (\prod_{U_i \in SG} y_i)^K \mod p). \tag{24}
\]

Step 3: The recipient \( U_r \) verifies
\[
K = h(g^S (\prod_{U_i \in SG} y_i)^K \mod p), M). \tag{25}
\]

If Eq. (25) holds, the signature is accepted; otherwise it is refused.

C. Signature Conversion (SC) Phase

If dispute on repudiation, the recipient \( U_r \) can release the \( \{S, K\} \) for the message \( M \). With this converted signature, anyone can validate its validity by Eq. (25).

IV. ANALYSIS OF THE IMPROVED SCHEME

Security analysis and computational complexity analysis of our improved scheme are given below.

A. Security Analysis

The security of the proposed scheme is based on well-known cryptographic assumptions: solving the discrete logarithm problem (DLP) [17] and the intractability of reversing the one-way hash function (OWHF) [18]. In the following, we discuss some possible attacks against the proposed scheme and show that the proposed scheme is secure under the protection of the DLP and OWHF assumptions.

1) Can the attacker reveal the secret key \( x_i \) of the signer \( U_i \in SG \) or the secret key \( x_v \) of the designated recipient \( U_v \) from all public information?

With the authenticated encryption signature \( \{S, C_1, C_2, Q\} \), \( x_i \) and \( x_v \), the attacker cannot derive the signer’s secret key \( x_i \) from Eq. (16), since the equation contains two unknown variables \( x_i \) and \( w_1 \), and \( w_1 \) is protected under the DLP assumptions. Similarly, the attacker cannot reveal verifier’s secret key \( x_v \) from Eq. (22) and Eq. (23), since \( x_v \) is protected under the DLP assumptions.

2) Can the attacker forge an authenticated encryption signature?

To forge a signature for satisfying Eq. (24), the attacker must know the all random numbers \( w_i \)’s and \( U_i \)’s private key \( x_i \). However, it will not be workable since all \( w_i \)’s and \( x_i \) are protected under the DLP assumption. The attacker cannot get them, because \( w_i \) and \( x_i \) are only hold by the signer \( U_i \in SG \). Thus, it is impossible for any attacker to forge the digital multi-signature of the message \( M \).

3) Can the attacker forge a converted signature?

If an adversary wants to forge a signature \( \{S, K\} \) of the message \( M \), this adversary must know the random number \( w_i \), \( U_i \)’s private key \( x_i \), the message \( M \) and \( R \). Assume that this adversary is an insider. He cannot get them, because the \( w_i \) and \( x_i \) are only hold by the signer \( U_i \), and \( R \) is the authenticated message for the message \( M \). Assume that this adversary is an insider. He cannot get the \( w_i \) and \( x_i \), because the \( w_i \) and \( x_i \) are only hold by \( U_i \). Thus, it is impossible for any adversary to forge the digital multi-signature of the message \( M \).

4) Can the attacker recover the message from the authenticated encryption signature?

With the authenticated encryption signature \( \{S, C_1, C_2, Q\} \), the attacker cannot derive the message \( M \) from Eq. (25) since the \( K \) is protected under the DLP assumption. In addition, the \( x_v \) is only hold by the signer \( U_v \). The attacker cannot derive the \( R \) from Eq. (22). Thus, it is impossible for an attacker to recover the message \( M \) from the Eq. (24) successfully.

<table>
<thead>
<tr>
<th>Phases</th>
<th>Our proposed scheme</th>
<th>Tsai’s scheme [2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>SE</td>
<td>Time complexities</td>
<td>(n^2+25m+1)T_{MUL}</td>
</tr>
<tr>
<td></td>
<td>Rough Estimation</td>
<td>(n^2+725m+1)T_{MUL}</td>
</tr>
<tr>
<td>MRV</td>
<td>Time complexities</td>
<td>T_H + (n+1)T_{MUL}</td>
</tr>
<tr>
<td></td>
<td>Rough Estimation</td>
<td>(n+734)T_{MUL}</td>
</tr>
<tr>
<td>SC</td>
<td>Time complexities</td>
<td>T_H + n_{MUL} + 2T_{Exp}</td>
</tr>
<tr>
<td></td>
<td>Rough Estimation</td>
<td>(n+494)T_{MUL}</td>
</tr>
<tr>
<td>Total</td>
<td>Time complexities</td>
<td>(n^2+327n+4227)T_{MUL}</td>
</tr>
<tr>
<td></td>
<td>Rough Estimation</td>
<td>(n^2+728n+1229)T_{MUL}</td>
</tr>
</tbody>
</table>

5) Can the attacker verify the signature before converted?

It requires the message \( M \) to perform the signature verification of Eq. (25). From the discussion (4), the attacker cannot obtain the message \( M \) before the signature is converted. Hence he cannot verify the signature.

B. Computational Complexity Analysis

We denote the following notations to facilitate the performance evaluation:

- \( T_{MUL} \): time for performing a modular multiplication computation,
- \( T_{Exp} \): time for performing a modular exponentiation computation,
- \( T_{H} \): time for performing a one-way hash function computation,
- \( T_{Inv} \): time for performing a modular inversion computation.

The time for performing the modular addition and the exclusive OR (XOR) operation are ignored, since they are relatively smaller than those for performing other operations. From [19], [20], the time complexities can be respectively regarded as \( T_{Exp} = 240 \ T_{MUL} \), \( T_{Inv} = 10 \ T_{MUL} \), and \( T_{H} = 4 \ T_{MUL} \). The performance evaluations of the two schemes are relatively smaller than those for performing other operations.
Fig. 8 shows the evolution stability with different proportion of initial cooperative groups in the wireless networks. It indicates the impact of different initial ratios of cooperative groups in $M_1$ and $M_2$ on the evolution of wireless networks speed. Set the initial value to $X = 0.5$, $X = 0.9$, $X = 0.1$, $Y = 0.5$, $Y = 0.9$, $Y = 0.1$ respectively, and assume $p(T_1-M_1) = 0.5$, as can be seen from Fig. 8, with the initial ratio of choosing cooperative jamming strategy in $M_1$ increasing, the speed of reaching evolving stability of group $M_2$ becomes faster. Conversely, with the initial ratio of choosing cooperative jamming strategy in $M_1$ decreasing, the speed of reaching evolving stability of group $M_1$ becomes lower.

V. CONCLUSION

In the wireless network with the presence of an eavesdropper, the transmitters tend to choose uncooperative strategy according to the approaches based on the classic game, resulting in that the secrecy rate of network cannot be further improved. In this paper, we propose cooperative interference based on evolutionary game in wire-tap channel. In this way, transmitters can cooperate with each other, and the network is evolution from an unstable state to a stable cooperative state to improve the secrecy rate of the system. The simulations results indicate that in the random Gaussian wire-tap channel, when cooperation becoming the only evolving stable strategy, the proposed approach can guarantee the security of communication, thus, the secrecy rate of whole network is improved.

REFERENCES


Kai-Zhi Huang was born in 1973. She received her Ph.D. degree in communication and information system from Tsinghua University. She is currently a professor and supervisor of postgraduate student. Now, she is the assistant director of mobile communication Department for National Digital Switching System Engineering &Technological R&D Center. Dr. Huang is serving as a leader of Henan “wireless mobile communication innovation technology team” and “excellent technology innovation group of General Staff Headquarters”. Her research interests include wireless mobile communication network and information secrecy.