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 [5] 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

Manuscript received January 20, 2014; revised March 23, 2014. This work was supported by National Natural Acience Fund of China (No. 61379006).

The authors are with the National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China (e-mail: huangkaizhi@tsinghua.org.cn, hongyinghunan@126.com, 13803853365@139.com).

DOI: 10.7763/IJFCC.2014.V3.317

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_1, if T_2 chooses no cooperation, because $R_1^i(r_2,r_2) > R_1^i(r_1,r_2)$, so T_1 chooses no cooperation to get a higher security rate. If T_2 chooses cooperation, T_1 also chooses no cooperation that to get a high security rate. So, no cooperation is the dominant strategy for T_1. Similarly, for T_2, 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 will get the cooperation benefit from other transmitter.

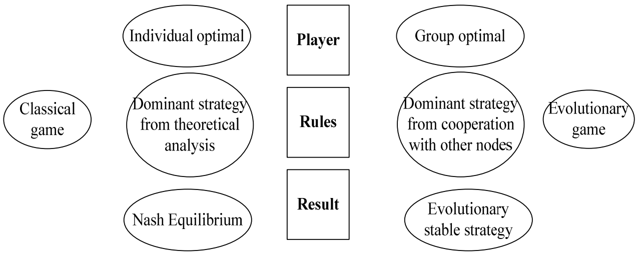
Individual optimal
Player
Group optimal
Classical game
Dominant strategy from theoretical analysis
Rules
Dominant strategy from cooperation with other nodes
Evolutionary game
Nash Equilibrium
Result
Evolutionary stable strategy

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_1 is given as X and the non-cooperative ratio is given as $1-X$. While the cooperative ratio in M_2 is given as Y and the non-cooperative ratio is given as $1-Y$. Then the average expected benefit is defined as

$$\bar{E}_{M_1} = XE_1^{M_1} + (1-X)E_2^{M_1} \tag{12}$$

$$\bar{E}_{M_2} = YE_1^{M_2} + (1-Y)E_2^{M_2} \tag{13}$$

where $E_1^{M_1}$, $E_1^{M_2}$ and $E_2^{M_1}$, $E_2^{M_2}$ denote the expected benefit function of cooperative strategy and no cooperative strategy.

The probability of T_1 belonging to M_1 is p and the probability of T_1 belonging to M_2 is q. Let $q=1-p$. Then we will get four kinds of networking strategy in M_1: (M_1 cooperation, M_1 cooperation), (M_1 cooperation, M_1 no cooperation), (M_1 cooperation, M_2 cooperation), (M_1 cooperation, M_2 no cooperation). Finally, we get the average expected benefit of cooperation in M_1:

$$E_1^{M_1} = p^2(XR_1^{r_1,r_1} + (1-X)R_1^{r_1,r_2})_{h_1>1,h_2>1} + pq(YR_1^{r_1,r_1} + (1-Y)R_1^{r_1,r_2})_{h_1>1,h_2<1} \tag{14}$$

Similarly, the average expected benefit of no cooperation in M_1 is

$$E_2^{M_1} = p^2(XR_1^{r_2,r_1} + (1-X)R_1^{r_2,r_2})_{h_1>1,h_2>1} + pq(YR_1^{r_2,r_1} + (1-Y)R_1^{r_2,r_2})_{h_1>1,h_2<1} \tag{15}$$

The average expected benefit of cooperation in M_2 is

$$E_1^{M_2} = q^2(YR_1^{r_1,r_1} + (1-Y)R_1^{r_1,r_2})_{h_1<1,h_2<1} + pq(XR_1^{r_1,r_1} + (1-X)R_1^{r_1,r_2})_{h_1<1,h_2>1} \tag{16}$$

The average expected benefit of no cooperation in M_2 is

$$E_2^{M_2} = q^2(YR_1^{r_2,r_1} + (1-Y)R_1^{r_2,r_2})_{h_1<1,h_2<1} + pq(XR_1^{r_2,r_1} + (1-X)R_1^{r_2,r_2})_{h_1<1,h_2>1} \tag{17}$$

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_1 is expressed as

$$dX/dt = X\left[E_1^{M_1} - \bar{E}_{M_1}\right] = X\left[E_1^{M_1} - XE_1^{M_1} - (1-X)E_2^{M_1}\right] \tag{18}$$

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_2 is expressed as

$$dY/dt = Y\left[E_1^{M_2} - \bar{E}_{M_2}\right] = Y\left[E_1^{M_2} - YE_1^{M_2} - (1-Y)E_2^{M_2}\right] \tag{19}$$

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

$(X(0),Y(0))\in[0,1]\times[0,1]$, $(X(0),Y(0))\in[0,1]\times[0,1]$, the transmitter random adopts a strategy in the initial state. Therefore, any point (X,Y) on the solution curve of inter-relay transmission dynamic replication network corresponds to a mixed strategy $(X\oplus(1-X),Y\oplus(1-Y))$. Clearly, the dynamic replication system has the following local stable point: $E_1(0,0)$, $E_2(1,0)$, $E_3(0,1)$, $E_4(1,1)$. These points represent the cooperative strategy proportion in M_1 and M_2, corresponding to the partial equilibrium state of the network.

B. Strategy Update for Cooperation

From the above analysis, when different strategies at the transmitters access the network, the other transmitter in the network will change their strategies, so that the state of the network is not absolutely stable. By constructing the Jacobian matrix of the replicator dynamics equation, this paper obtains the condition that cooperation becomes the only evolutionary stable strategy under certain wire-tap channel state information, making the whole network stable.

Theorem 3.1 the necessary and sufficient conditions for cooperation being the only evolutionary stable strategy is: When power is arbitrarily fixed value, the probability of T_1 belonging to M_1 meets $p<p^*$, p^* is the smallest value of $\frac{(R_1^{r_1,r_1})_{h_1<1,h_2<1}}{(R_1^{r_2,r_1})_{h_1<1,h_2>1}+(R_1^{r_1,r_1})_{h_1<1,h_2<1}-(R_1^{r_1,r_1})_{h_1<1,h_2>1}}$.

Proof: Existence

By formula (18) and (19), we can get the corresponding Jacobian matrix,

$$J=\begin{bmatrix} A & B \\ C & D \end{bmatrix} \tag{20}$$

where

$$A=(1-2X)\begin{pmatrix} p^2(XR_1^{r_1,r_1}+(1-X)R_1^{r_1,r_2})_{h_1>1,h_2>1} \\ +pq(YR_1^{r_1,r_1}+(1-Y)R_1^{r_1,r_2})_{h_1>1,h_2<1} \\ -p^2(XR_1^{r_2,r_1}+(1-X)R_1^{r_2,r_2})_{h_1>1,h_2>1} \\ -pq(YR_1^{r_2,r_1}+(1-Y)R_1^{r_2,r_2})_{h_1>1,h_2<1} \end{pmatrix}$$
$$+X(1-X)(p^2(R_1^{r_1,r_1}+R_1^{r_2,r_2})_{h_1>1,h_2>1})$$
$$C=Y(1-Y)(pq(R_1^{r_1,r_1}-R_1^{r_1,r_2})_{h_1<1,h_2>1}$$
$$-pq(R_1^{r_2,r_1}-R_1^{r_2,r_2})_{h_1<1,h_2>1})$$
$$B=X(1-X)(pq(R_1^{r_1,r_1}-R_1^{r_1,r_2})_{h_1>1,h_2<1}$$
$$-pq(R_1^{r_2,r_1}-R_1^{r_2,r_2})_{h_1>1,h_2<1})$$
$$D=(1-2Y)\begin{pmatrix} q^2(YR_1^{r_1,r_1}+(1-Y)R_1^{r_1,r_2})_{h_1<1,h_2<1} \\ +pq(XR_1^{r_1,r_1}+(1-X)R_1^{r_1,r_2})_{h_1<1,h_2>1} \\ -q^2(YR_1^{r_2,r_1}+(1-Y)R_1^{r_2,r_2})_{h_1<1,h_2<1} \\ -pq(XR_1^{r_2,r_1}+(1-X)R_1^{r_2,r_2})_{h_1<1,h_2>1} \end{pmatrix}$$
$$+Y(1-Y)(q^2(R_1^{r_1,r_1}+R_1^{r_2,r_2})_{h_1<1,h_2<1})$$

The necessary and sufficient conditions for cooperation being the only evolutionary stable strategy in the wireless network is $\det J>0$, $\operatorname{tr}J<0$. By substituting $(X=1,Y=1)$ into Jacobian J, we will obtain

$$J=\begin{bmatrix} E & 0 \\ 0 & F \end{bmatrix} \tag{21}$$

The determinant of the matrix is

$$\det J = EF>0 \tag{22}$$

The trace of the matrix is

$$\operatorname{tr}J=E+F<0 \tag{23}$$

As $\operatorname{tr}J=E+F$ is constant less than 0, when $\det J = EF$ is greater than 0, E is constant less than 0. Then $F=pq(R_1^{r_2,r_1})_{h_1<1,h_2>1}-q^2(R_1^{r_1,r_1})_{h_1<1,h_2<1}-pq(R_1^{r_1,r_1})_{h_1<1,h_2>1}<0$, we will obtain

$$p<p^*=\min(\frac{(R_1^{r_1,r_1})_{h_1<1,h_2<1}}{(R_1^{r_2,r_1})_{h_1<1,h_2>1}+(R_1^{r_1,r_1})_{h_1<1,h_2<1}-(R_1^{r_1,r_1})_{h_1<1,h_2>1}}) \tag{24}$$

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

Equilibrium Point(X,Y)	det J		tr J		Stability
(1,1)	>0	+	<0	-	ESS
(0,1)	=0		<0	-	Unstable
(1,0)	=0		<0	-	Unstable
(0,0)	=0		<0	-	Unstable

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 $E_1^{M_1}$, $E_1^{M_2}$ under cooperation and average expected benefits $\bar{E}_{M_1}$, $\bar{E}_{M_2}$.
4) According to the dynamic equation $dX/dt=X\left[E_1^{M_1}-\bar{E}_{M_1}\right]$, $dY/dt=Y\left[E_1^{M_2}-\bar{E}_{M_2}\right]$, M_1 and M_2 update the proportion X, Y of cooperative strategy.
5) We can get partial equilibrium point of the network by $dX/dt=0$, $dY/dt=0$.
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_v computes

$$R = C_2 \oplus C_1^{x_v} \bmod p\,, \tag{22}$$

$$K = Q \oplus C_1^{x_v} \bmod p\,. \tag{23}$$

Step 2: The recipient U_v recovers the message M by computing

$$M = R \oplus (g^S (\prod_{U_j \in SG} y_j)^{-K} \bmod p)\,. \tag{24}$$

Step 3: The recipient U_v verifies

$$K = h((g^S (\prod_{U_j \in SG} y_j)^{-K} \bmod p), M)\,. \tag{25}$$

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

C. Signature Conversion (SC) Phase

If dispute on repudiation, the recipient U_v 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 $\{S, C_1, C_{2,l}, Q\}$, s_i and r_i, 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_i, and w_i 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 here 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 outsider. 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 $\{S, C_1, C_{2,l}, Q\}$, 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 I: Comparisons of Computational Complexities

Phases		Our proposed scheme	Tsai's scheme [2]
SE	Time complexities	$nT_H + (3n)T_{EXP}$ $+ (n^2+n-1)T_{MUL}$	$nT_H + (3n)T_{EXP}$ $+ (n^2+2n-1)T_{MUL}$
	Rough Estimation	$(n^2+725n-1)T_{MUL}$	$(n^2+726n-1)T_{MUL}$
MRV	Time complexities	$T_H + (n+1)T_{MUL}$ $+ 3T_{EXP} + T_{INV}$	$T_H + (n+1)T_{MUL}$ $+ 3T_{EXP} + T_{INV}$
	Rough Estimation	$(n+734)T_{MUL}$	$(n+735)T_{MUL}$
SC	Time complexities	$T_H + nT_{MUL}$ $+ 2T_{EXP} + T_{INV}$	$T_H + (n+1)T_{MUL}$ $+ 2T_{EXP} + T_{INV}$
	Rough Estimation	$(n+494)T_{MUL}$	$(n+495)T_{MUL}$
Total	Time complexities	$(n+2)T_H + 2T_{INV}$ $+ (n^2+3n-1)T_{MUL}$ $+ (3n+5)T_{EXP}$	$(n+2)T_H + 2T_{INV}$ $+ (n^2+4n+1)T_{MUL}$ $+ (3n+5)T_{EXP}$
	Rough Estimation	$(n^2+727n+1227)T_{MUL}$	$(n^2+728n+1229)T_{MUL}$

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 $T_{EXP} \approx 240\ T_{MUL}$, $T_{INV} \approx 10\ T_{MUL}$, and $T_H \approx 4\ T_{MUL}$. The performance evaluations of the two schemes are

Fig. 8 shows the evolution stability with different proportion of initial cooperative groups in the wireless networks. It indicates the impaction 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. 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_2 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

[1] P. Gupta and P. Kumar, “The capacity of wireless networks,” *IEEE Trans. on Information Theory*, vol. 46, no. 2, pp. 388-404, 2000.

[2] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[3] R. Liu, I. Maric and P. Spasojevic, “Discrete Memoryless Interference and Broad- cast Channels with Confidential Messages: Secrecy Rate Regions,” *IEEE Trans. on Information Theory*, vol. 54, no. 6, pp. 2493-2507, 2008.

[4] R. Q. Zhang and L.Y Song, “Physical layer security for two-way untrusted relaying with friendly jammers,” *IEEE Trans. on Vehicular Technology*, vol. 61, no. 8, pp. 3693-3704, 2012.

[5] J. Zhou, “Wiretap channel based on game theory in security research,” M.S. Thesis, Dept. Communication, Nangjing Posts and Telecommunications Univ., Nangjing, China, 2013.

[6] A. K. Manzoor, T. Hamidou, and V. Athanasios, “Evolutionary coalitional games: design and challenges in wireless networks,” *IEEE Trans. on Wireless Communications*, vol. 19, no. 2, pp. 50-56, 2012.

[7] S. Walid, X.Y. Zhang and M. Behrouz, “Tree Formation with Physical Layer Security Considerations in Wireless Multi-Hop Networks,” *IEEE Trans. on Wireless Communications*, vol. 11, no. 11, pp. 3980-3991, 2012.

[8] Z. Chen, “Research on the evolution of dynamic network,” M.S. thesis, Dept. Communication, SJTU Univ., Shanghai, China, 2012.

[9] D. L. Lu, “Research on the evolution of dynamic network”, M.S. thesis, Dept. Communication, Soochow Univ., Suzhou, China, 2012.

[10] S. Goel and R. Negi, “Guaranteeing secrecy using artificial noise,” *IEEE Trans. on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, 2008.

[11] Y. C. Leung and M. Hellman, ‘The gaussian wire-tap channel,” *IEEE Trans. on Information Theory*, vol. 24, no. 4, pp. 451-456, 1978.

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.