Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 9437936, 13 pages
https://doi.org/10.1155/2018/9437936

Research Article

A Rational Exchange Protocol under Asymmetric Information in Wireless Sensor Networks

Zhen Lv,[1] Changgen Peng,[2] Yanguo Peng,[3] and Junwei Zhang[4]

[1]*Department of Basic Sciences, Air Force Engineering University, Xi'an 710051, China*
[2]*Guizhou Province Key Laboratory of Public Big Data, Guizhou University, Guiyang 550025, China*
[3]*School of Computer Sciences and Technology, Xidian University, Xi'an 710071, China*
[4]*School of Cyber Engineering, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Yanguo Peng; ygpeng@xidian.edu.cn

Received 7 March 2018; Revised 22 April 2018; Accepted 30 April 2018; Published 31 May 2018

Academic Editor: Kim-Kwang Raymond Choo

P2P network is one of the most extensive network frameworks for wireless sensor network (WSN) in Internet of Things (IoT). The peers in WSN are rational and often free ride to save power of electricity and calculation, due to the fact that the usability is of great variability and unpredictability. Such a phenomenon tremendously reduces the quality of service (QoS) in WSN. Rational exchange protocol aims at promoting QoS and guaranteeing security and fairness. However, existing schemes have taken only complete information into account, which is not up to realistic environment. The peers in realistic environment indeed possess incomplete information, which is, however, still not thoroughly investigated so far. In this paper, under asymmetric information (a typical incomplete information), an entropy based incentive model is well designed based on Markov model and QoS evaluation model to help peers cooperate in WSNs. A concrete utility function with entropy is constructed to evaluate decision utility in P2P network. Finally, an entropy based rational exchange protocol is proposed based on the presented incentive model and concrete utility function, with analysis of correctness, security, fairness, and robustness, respectively. The proposed protocol can facilitate rational peers positively and sensibly participating in services and prevent free riding for rational peers. Hence, it further promotes QoS and guarantees security and fairness simultaneously in WSNs.

1. Introduction

Wireless sensor network (WSN) contains massive static and dynamic wireless sensors that extremely lack electricity and calculation. Due to that, sensors are highly willing to intentionally free ride [1–4] for better efficiency selfishly. Especially, in P2P network, which is one of the most extensive network frameworks for WSNs, peers (i.e., wireless sensors) are rational in fact. Rational peers make decisions to maximize their own benefit first and tremendously reduce the quality of service (QoS) of WSNs. To prevent free riding of rational peers and promote QoS, rational protocols have been widely investigated in security community [5–8].

Rational cryptography is a fresh and important branch in cryptographic research field, where rational exchange protocol is compatible and applicable for WSNs. Rational exchange protocol, which promotes peers to positively provide various services (data transmitting, data sharing, data distributing, etc.), aims at promoting QoS in WSNs. Simultaneously, rational exchange protocol guarantees both security and fairness for peers in WSNs, which are practical and necessary requirement in realistic environments.

Existing rational exchange protocols have been widely investigated since they were proposed by Syverson [9] in 1998. After that, extensive research work has been done under complete information [10–14], which means that each peer in WSN is fully aware of characteristics of participants, strategic space, and utility function about others. In realistic environments, however, the information is not always available (type, reputation, QoS, etc.), in which information is incomplete. A typical phenomenon is under asymmetric information [15], where, between two communicating peers, one possesses private information while the other is not aware of that. Unfortunately, rational exchange protocol under asymmetric

information is not well considered so far and should be investigated thoroughly.

We focus on, in this paper, proposing a rational exchange protocol with security and fairness under asymmetric information. Also, it is applied in wireless sensor networks aiming at promoting QoS of peers. The dominating contributions are as follows.

(1) To quantify utilities of participants, a dynamic game model with entropy is presented. In such a model, the utility for participants can be quantitatively analyzed. Furthermore, a selective basis of strategies in a game is explicitly provided (Section 2.1).

(2) Under asymmetric information, a Markov-based entropy function and a QoS evaluation model are designed. A utility function with entropy is further concreted to measure fairness of rational exchange protocol (Section 3).

(3) A concrete rational exchange protocol under asymmetric information is presented with through analysis of correctness, security, fairness, and robustness. Additionally, the proposed utility function with entropy is simulated and appropriateness is declared (Section 4).

The rest of this paper is organized as follows. Section 2 introduces the problem definition and preliminaries. Under asymmetric information, Section 3 presents a utility function with entropy based on Markov-based entropy function and QoS evaluation model. The concrete rational exchange protocol is proposed in Section 4 with thorough analysis. The simulation of utility function with entropy is presented in Section 5. Finally, the related work is summarized in Section 6 and this paper is concluded in Section 7.

2. Problem Definition and Preliminaries

In this section, we formally define a dynamic game model in which a utility function with entropy can be derived. Following that, a rational exchange protocol is formalized.

For facile understanding, the primary notations are listed in Table 1.

Table 1: Primary notations.

Notation	Meaning
$\mathbb{P}, P_i$	Set of participants and participant.
n	Number of participants in $\mathbb{P}$.
inf	Exchanging Information.
A	Set of optional actions.
$H(\bullet)$	Mixed strategy entropy function.
T	Participant's contribution value.
c	Unitary cost for participating in an exchange.
w_{ij}	Credit that participant P_j rates P_i.
Z	Participant's number of positive feedbacks.
U	Utility.
$\mathtt{T}$	Transfer matrix of participant's type.
$\mathtt{R}$	Possibility matrix of service for all participants.
PUB	Bulletin board.
$E(), D()$	Asymmetric encryption and decryption functions.
$\widehat{E}(), \widehat{D}()$	Symmetric encryption and decryption functions.
$\omega(x)$	Weakly secret bit commitment function.
PK, SK, k	Public key, private key, and session key.

2.1. Definition of Dynamic Game with Entropy. In this section, a dynamic game model with entropy is introduced to pave the way to quantify utilities of participants.

Definition 1 (dynamic game model with entropy). A dynamic game model with entropy contains a seven-tuple $\{\mathbb{P}, Q, (I_i)_{P_i\in\mathbb{P}}, A, f_p, (\geq_i)_{P_i\in\mathbb{P}}, (H_i(\bullet))_{P_i\in\mathbb{P}}\}$, where the elements are formally defined as follows.

(i) $\mathbb{P}$ is a set of participants, in which p_i is a participant.

(ii) Q is a set of sequences of actions containing all participants' actions. A sequence consists of participant's specific actions in a dynamic game. Q satisfies the following characteristics.

(1) The empty sequence is $\emptyset \in Q$.

(2) If a sequence of actions q satisfies that $q = (a_j)_{j=1}^{w} \in Q$ and $0 < v < w \in N^*$, then $q' = (a_j)_{j=1}^{v} \in Q$ holds.

(3) If any $v \in N^*$ and $q' = (a_j)_{j=1}^{v} \in Q$ holds, then the infinite sequence of actions $q = (a_j)_{j=1}^{\infty} \in Q$ holds.

(iii) $(I_i)_{P_i\in\mathbb{P}}$ is participant P_i's information set denoting the previous information of other participants in a game. An information set is formally denoted as $(I_i)_{P_i\in\mathbb{P}} = \{x_1, x_2, \ldots, x_m\}$, where x_i is the previous m action sequences of the other participants and the corresponding probability distribution is $\{p(x_1), p(x_2), \ldots, p(x_m)\}$ such that $\sum_{i=1}^{m} p(x_i) = 1$.

(iv) A is a set of optional actions, in which $A = \cup A_i$ and A_i is the optional actions of participant P_i.

(v) f_p is a participant function, to determine the next participant of nonterminal sequence of actions.

(vi) $(\geq_i)_{P_i\in\mathbb{P}}$ is a preference relation for participant P_i under a set of mixed strategies. Generally, the utility function $U_i(q)$ of participant P_i is the preference. The preference relation $q^* \geq_i q$ means that $U_i(q^*) \geq U_i(q)$ and q^* is the willing action sequence for participant P_i.

(vii) $(H_i(\bullet))_{P_i\in\mathbb{P}}$ is a mixed strategy entropy function for participant P_i. It is a probability distribution function of strategies on $(I_i)_{P_i\in\mathbb{P}}$. Given the round number r of a game, the entropy function of participant P_i in rth round is $H_i(r) = -\sum p(x_i) \log p(x_i)$, in which $H_i(\bullet) = \sum_{r=1}^{N} H_i(r) \geq 0$ is the total entropy of participant P_i during a whole game.

So far, we define a novel dynamic game model to analyze the rational exchange protocol that will be proposed in the following.

2.2. Definition of Rational Exchange Protocol. In this paper, rational exchange protocol is thoroughly investigated under two participants. Such a protocol can be facilely generalized into multiple participants in theory.

Definition 2 (rational exchange protocol with entropy). A rational exchange protocol with entropy contains a five-tuple $\{H(X \mid Y), P_A, P_B, PUB, \pi\}$, in which $H(X \mid Y)$ is a conditional entropy, P_A and P_B are the participants, PUB is a bulletin board, and π is the concrete exchange protocol. Additionally, π is formally defined as follows.

(i) *Setup*: generate the secret and public keys for P_A and P_B and other public parameters.

(ii) *Rational exchange*: participants P_A and P_B own information inf_A and inf_B, respectively. P_A and P_B rationally exchange their information, which means that P_A and P_B correctly get inf_B and inf_A, respectively, or get nothing.

A rational exchange protocol must satisfy the following four pivotal requirements.

Correctness. Such a requirement provides a guarantee that, when π is finished, P_A and P_B can successfully exchange inf_A and inf_B. Additionally, both P_A and P_B receive the positive feedbacks and credits that are defined later, in time.

Security. Both inf_A and inf_B must be prevented from adversary's cracking. That means there is no illegal participant that can derive anything from encrypted information during the exchange. Additionally, such a protocol can not reveal anything valuable during interactive processes.

Fairness. Since all participants are rational and aim at maximizing their own benefit, a rational exchange protocol is fair when the expected utilities for all the participants are maximized.

Robustness. The protocol is steady. That means even when the protocol is destabilized or interrupted, the fairness is still satisfied.

3. Utility Function with Entropy under Asymmetric Information

Before designing and representing a formal rational exchange protocol, a utility function capability for the dynamic game model with entropy is proposed in this section. Specifically, a Markov-based entropy function and a QoS evaluation model under asymmetric information are sequentially designed. Based on both of them, a utility function with entropy is concreted under asymmetric information.

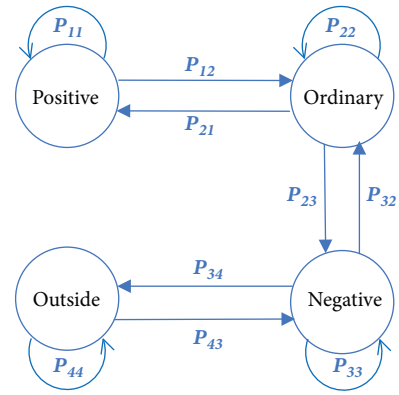


Figure 1: The transfer types for participants.

3.1. Markov-Based Entropy Function. Under asymmetric information, participant does not completely know, before exchanging information, about other participants' a priori information (i.e., participant's type). Additionally, participant's status relies only on the last past status. Hence, we introduce Markov chain to evaluate participant's information entropy.

Participants in our model are categorized into four types according to the contribution of participant in the system.

(i) *Positive*: such a participant provides service with a higher probability (e.g., $p \geq 80\%$). Here, positive participant's QoS is preferable. He can transfer to be ordinary.

(ii) *Ordinary*: such a participant provides service with a moderate probability (e.g., $50\% \leq p < 80\%$). He can transfer to be positive or negative.

(iii) *Negative*: such a participant provides service with a lower probability (e.g., $0\% < p < 50\%$). He can transfer to be ordinary or outside.

(iv) *Outside*: such a participant does not provide any service (e.g., $p = 0\%$) and does always free ride. He can transfer to be only negative.

In the transfer, each participant stays in a specific type with a specific probability and each transfer occurs with a specific probability too. The transfer between participants with different types is illustrated in Figure 1.

The constraint rules for participant's action are as follows.

(1) Allow participant to be outside when he first participates in a game.

(2) Every other period with time $t > 0$, the mechanism figures out the distribution of all participants' types.

By following the above constraints, every period, the probability R_{ij} for participant P_j serving participant P_i is estimated based on Markov chain. Based on the distribution in Step (2), the transfer matrix $\mathtt{P}_{4\times4}$ of participants' types can be resolved. Specifically, at jth period, the transfer matrix is $\mathtt{P}^{[j]} = \mathtt{P}(0) \bullet \mathtt{P}^j$, and the steady-state vector $\mathtt{D}$ is derived by resolving a system of linear equations $\mathtt{D} = \mathtt{D} \bullet \mathtt{P}$. Here,

$\mathtt{D} = (\mathtt{d}_i)_{i=1,2,3,4}$. The probability of service is $R_{ij} = \mathtt{D} \bullet \mathtt{g}^T$, where $\mathtt{g} = (\mathtt{g}_i)_{i=1,2,3,4}$ is the vector containing all membership functions corresponding to all participants' types (i.e., by embedding membership functions, the values of probabilities that participant provides service can be estimated in advance; thus, participant will be further convinced of his decision). In our construction, $\mathtt{g}_i$ $(1 \le i \le 4)$ stands for the tendency of maintaining a specific type (positive, ordinary, negative, and outside) for a participant. Finally, the probability matrix of service for all participants is $\mathtt{R}_{n\times n} = \{R_{ij}\}$, where $1 \le i, j \le n$.

According to the analysis of Shannon entropy and perceptive information, when a system achieves steady, P_i's total quantity of services coming from other participants is $H_i = -\sum_{j=1}^{n} R_{ij} \ln R_{ij}$, where $i \ne j$. From the aspect of expectation, H_i is larger; also P_i's willingness to participate in exchanging information is stronger. The expectation for the whole system is $H = \sum_{P_i \in \mathbb{P}} H_i$, which is changing with periods.

The ultimate entropy H_∞ of m-orderly discrete information source with memory is the m-orderly conditional entropy for a steady system. That means $H_\infty = \lim_{n\to\infty} H(X_n \mid X_1 \dots X_{n-1}) = H(X_{m+1} \mid X_1 \dots X_m) = H_{m+1}$, in which $H_{m+1} = -\sum_{i=1}^{n} \sum_{j=1}^{n} R_{ij} \ln R_{ij}$. The ultimate entropy H_∞ weighs the average quantity of information of all symbols that the information source sends. That means all the participants in an exchange protocol achieve steady.

3.2. QoS Evaluation Model under Asymmetric Information. Asymmetric information is a typically incomplete information. It means that, in an exchange protocol, a participant's information is complete, and the other's is incomplete. The former is advantageous participant, and the latter is disadvantageous participant. A rational participant makes decision through observing information that other participants reveal and deducing other participants' actions, in order to make his own expected utility maximum.

In this section, a deducing method is presented to turn asymmetric information into weakened-symmetric information. Based on that, a QoS evaluation model under asymmetric information is proposed for guaranteeing disadvantage and advantageous participants' fairness simultaneously.

For a disadvantageous participant (i.e., receiver) and an advantageous participant (i.e., sender) in a rational exchange protocol, the receiver derives a random variable Y about the exchanging information according to his own prior knowledge. The realistic information X is estimated by Y. In such a case, $H(X \mid Y)$ is the uncertainty of X on the condition that Y is known. Here, let $H(X)$ be the prior uncertainty and $H(X \mid Y)$ be the posterior uncertainty. The mutual information entropy is $H(X;Y) = H(X) - H(X \mid Y)$, which stands for the average quantity of information that is derived from Y about X. If $H(X \mid Y) \to 0$, then $H(X;Y) \to H(X)$ and asymmetry of two participants is removed. The random variable Y can be corrected according to Bayes rules with exchanging information. The transform process is shown in Figure 2.

Let $H_q(\bullet) = H(X)$ be the quantity of exchanging information that the receiver does not know. To overcome

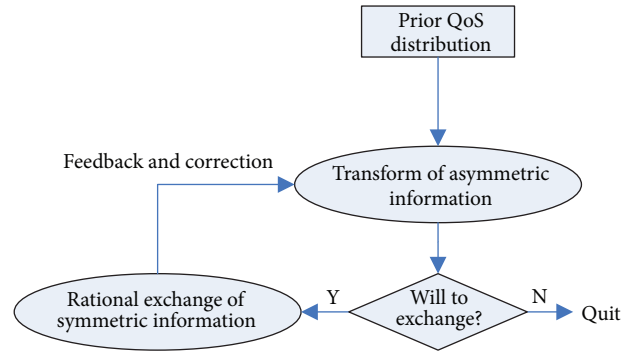


Figure 2: The transform process from asymmetric information to symmetric information.

the asymmetry of information, in fact, the receiver corrects service quantity by Bayes probability principle $p(x \mid y) = p(y \mid x)p(x)/p(y)$ with other participants' valuation about the exchanging information and derives the posterior probability distribution $\widehat{\pi}_q$.

Definition 3 (QoS evaluation mechanism). In a QoS evaluation mechanism, a list is maintained along with a whole rational exchange protocol. For participant P_i, the element in the list contains a three-tuple $\{P_i, Z_i, RP_i\}$. Here, P_i is the unique identifier, Z_i is the number of positive feedbacks, $RP_i = \cup_{l=1}^{m} \{A_{il}, \delta_{il}, (w_{ij})_{P_j \in \mathbb{P}\setminus\{P_i\}}\}$ is the set of records for lth round, in which A_{il} is the set of lth round actions, δ_{il} is the comment about quality of information in lth round, and $(w_{ij})_{P_j \in \mathbb{P}\setminus\{P_i\}}$ is the vector of credits for lth round information exchange.

Specifically, the list above is maintained at a bulletin board. After lth round exchange between sender P_S and receiver P_R, the following steps are carried out.

(1) P_R comments on such an exchange and uploads δ_{Sl} to the bulletin board. The bulletin board records actions in this exchange as A_{Sl}.

(2) P_R rates the quality of the exchanged information as w_{SR} and uploads it to the bulletin board.

(3) P_R can make a positive feedback by setting $Z_S = Z_S + 1$ if w_{SR} is greater than a threshold and a negative feedback by setting $Z_S = Z_S - 1$ if w_{SR} is smaller than a threshold.

(4) If there are multiple receivers $P_j \in \mathbb{P}\setminus\{P_R\}$ $(1 \le j \le m)$ in the system, P_j rates the quality of the exchanged information as w_{Sj} and makes a positive feedback for the other participants who make a consistent credit w_{Sj}.

By embedding such a QoS evaluation mechanism, all participants are further more willing to really evaluate the quality of exchanged information, in order to maximize credit and number of positive feedbacks. It is vital to measure participant's long-term utility.

3.3. Utility Function with Entropy. By comprehensive consideration of long-term utility and short-term utilities, the utility function with entropy is proposed for participant P_i.

$$U_i = -c_i T_i + H_i \left(\sum_{j=1}^{n} w_{ij} + \ln Z_i \right) T_i. \quad (1)$$

Here, c_i is the unitary cost for participating in an exchange and obtaining a unitary contribution value. $T_i = \alpha \sum_{j=1}^{n} R_{ij}$ is the contribution value in which the contribution weight α falls in $(0, 1)$.

In the equation, w_{ij} reflects short-term benefit and Z_i reflects long-term benefit for participant. In fact, in realistic scenarios, short-term benefit is more crucial than long-term benefit. In order to respond to such a correlation, it is necessary to take the logarithm of Z_i in the equation. By logarithm, the protocol is able to prevent participants with long-term benefit doing one-time deceive and provides rational fair from a new point of view. Through the combination of both, the utility function is more practical than others proposed in existing schemes.

Additionally, the product of information entropy H_i, which is the quantization of QoS, and $\sum_{j=1}^{n} w_{ij} + \ln Z_i$ constitutes the unitary revenue. Furthermore, T_i multiplied by $H_i(\sum_{j=1}^{n} w_{ij} + \ln Z_i)$ is P_i's revenue. According to the definition, $c_i T_i$ is the cost in total. Hence, the eventual utility for participant P_i is formalized and quantized by (1).

4. The Rational Exchange Protocol

In this section, the proposed concrete rational exchange protocol under asymmetric information is presented at the beginning. Following that, the detailed analysis is thoroughly stated. Additionally, theoretical comparisons between rational exchange protocols are represented to declare the presented rational exchange protocol's superiority.

4.1. Construction. Assume that there is no trusted third party in the proposed rational exchange protocol with multiple participants. That means each participant makes decision by maximizing his utility. Such a participant is rational and enjoys equal status, without considering compromising between participants.

In the concrete protocol, any two participants directly exchange information with each other. Assume that a sender P_A and a receiver P_B exchange inf_A and inf_B in the rational exchange protocol. Under asymmetric information, P_A is the advantageous participant and P_B is the disadvantage one. Additionally, inf_A is channel-sensitive and takes a long time t to be transmitted, but the time to transmit inf_B is short and negligible. There is also a bulletin board in the protocol to only manage all participants' account information and nothing else.

Setup. A weakly secret bit commitment function $\omega(x)$ is adopted, in which x can only be derived over time $t_0 > t$ since it is encrypted. An asymmetric encryption algorithm E and a symmetric encryption algorithm $\widehat{E}$ are adopted.

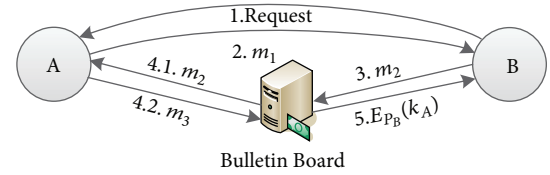


Figure 3: The concrete rational exchange protocol.

The corresponding decryption algorithms are D and $\widehat{D}$. According to the adopted asymmetric encryption algorithm E, $\langle PK_A, SK_A \rangle$ is generated for participant P_A as the public-private key pair, and $\langle PK_B, SK_B \rangle$ is generated for participant P_B too. Additionally, the bulletin board PUB is initialized by maintaining QoS evaluation mechanism with an empty list.

Rational Exchange. P_A and P_B rationally exchange information inf_A and inf_B by executing the following steps. The interactive processes for two participants are illustrated in Figure 3.

(1) The disadvantageous participant P_B calculates the conditional entropy $H(X \mid Y)$ according to the advantageous participant P_A's number of positive feedbacks Z_A. He makes decision by checking $H(X \mid Y)$. If he wishes to exchange information, then he continues to do the following steps. Otherwise, the protocol halts.

(2) P_A randomly chooses a session key k_A for $\widehat{E}$ and sends m_1 to P_B, in which $m_1 = E_{PK_B}(E_{SK_A}(B, \widehat{E}_{k_A}(inf_A)), B, \widehat{E}_{k_A}(inf_A))$.

(3) After receiving $m_1 = E_{PK_B}(Y_1, Y_2, Y_3)$, P_B decrypt m_1 and derive $B = Y_2$ and $\widehat{E}_{k_A}(inf_A) = Y_3$ by checking $D_{PK_A}(Y_1) = (Y_2, Y_3)$. If $D_{PK_A}(Y_1) = (Y_2, Y_3)$ does not hold, then P_B halts. Otherwise, P_B randomly chooses a session key k_B for $\widehat{E}$ and sends m_2 to PUB, in which $m_2 = E_{PK_A}(E_{SK_B}(A, \widehat{E}_{k_B}(inf_B), \omega(k_B)), A, \widehat{E}_{k_B}(inf_B), \omega(k_B))$. Such a process provides an evidence for possible disputation in future.

(4) A downloads $m_2 = E_{PK_A}(Y_1, Y_2, Y_3, Y_4)$ from the bulletin board PUB. P_A derives $A = Y_2$, $\widehat{E}_{k_B}(inf_B) = Y_3$, and $\omega(k_B) = Y_4$ by decrypting m_2. If $D_{PK_B}(Y_1) = (Y_2, Y_3, Y_4)$ does not hold, then P_A halts. Otherwise, P_A sends m_3 to PUB and P_B simultaneously, in which $m_3 = (\omega(k_B), E_{PK_B}(E_{SK_A}(B, k_A), B, k_A))$.

(5) After receiving $m_3 = (Y_1, E_{PK_B}(Y_2, Y_3, Y_4))$, if $D_{PK_A}(Y_2) = (Y_3, Y_4)$ does not holds, P_B sends m_3 and k_A to PUB. Then, PUB checks the validation of received information from P_B. If the information is valid, PUB marks inf_B invalid and rates a negative feedback for P_A according to the QoS evaluation mechanism proposed in Section 3.2. Additionally, the feedback information about P_A from other participants is also rated in a similar way.

According to the principle of long-term utility maximization for rational participants, rational participants will

not deceive others in a game. We analyze possible deceiving behaviors in the following.

Step (2). The possible deceiving is that P_A sends a fake inf_A. In such a case, in Step (5), P_B can verify the truth of inf_A and figure out the deceiving. Indeed, P_A can not deny such a deceiving. Meanwhile, $\omega(k_B)$ is still secretive and P_A still does not get inf_B. At the moment, P_B reports the deceiving of P_A to *PUB* and posts a negative feedback for P_A. *PUB* invalidates information inf_A and keeps a record. Other participants will deny the validation of inf_A. In this way, P_A does not get inf_B and indeed gets a serious negative feedback. In a long-term game, P_A will not send a fake inf_A ever.

Step (3). The possible deceiving, in this process, is that P_B sends a fake k_B. Due to the characteristics of $\omega(k_B)$, over time t_0, P_A can not derive inf_B using k_B. Other participants will also observe that P_B is deceiving and will not exchange anything else with P_B. In a long-term game, P_B's utility decreases dramatically, and hence he will not send a fake inf_B ever.

Step (4). P_A deceives P_B by not sending m_3 even over time t or sending a fake k_A. P_B can post a negative feedback for P_A and gain the supports from other participants. In such a case, P_A's utility is $U_A = -c_A T_A + H_A(\sum_{j=1}^{n} w_{Aj} + \ln Z_A)T_A$, in which $w_{AA} = 0$. Obviously, the loss of utility for P_A is great. Hence, P_A will not deceive in this process.

4.2. Theoretical Analysis. The correctness, security, fairness, and robustness of the proposed rational exchange protocol are analyzed, respectively, in this section.

Correctness. According to the concrete rational exchange protocol, the sender P_A finally receives inf_B and the corresponding rating w_{AB}. In one hand, the possible deceiving is that P_B send a fake session key $\widehat{k}_B$ to *PUB* in Step (3). In such a case, after a period t_0, all participants will observe the deceiving since $\omega(k_B)$ will be decrypted due to the inherent property of weakly secret bit commitment function. For long-term utility, P_B will also never do deceiving. On the other hand, due to the high relation between w_{AB} and Z_B, participant P_B will rate w_{AB} to acquire more positive feedbacks.

In the whole protocol, all participants are constrained by ratings and utility. In an exchange, specifically, Z_i is highly correlated to participant P_i's reputation and $H(X \mid Y)$ is prerequisite for participant to exchange information. For long-term utility, all participants are of high willingness to positively and honestly participate in an exchange. Hence, both Z_i and $H(X \mid Y)$ can prompt all participants to positively participate the protocol.

Hence, the protocol is correct.

Security. On one hand, security of the presented rational exchange protocol relies on the security of adopted asymmetric and symmetric encryption algorithms, which are assumed to be secure. Specifically, in Step (2), m_1 is in the encrypted form, whose security relies on the security of adopted encryption algorithms. It means that inf_A will not be revealed until the adopted encryption algorithms are breaking. In fact, there is no adversary that can break such algorithms. Hence, information in Step (2) is secure. Similarly, information in Step (3) and (4) is secure too.

Also, on the other hand, security relies on the interactive process during the whole protocol. In the following, the presented rational exchange protocol is proved to be secure under BAN logic [16]. For facile analysis, the presented rational exchange is formalized as follows. Note that Step (1) and (5) are not interactive and hence can be ignored in the analysis of security. However, it does not put any negative effect on security of the presented rational exchange protocol.

(2) $A \to B$: $\{\{\{inf_A\}_{k_A}\}_{SK_A}\}_{PK_B}$.
(3) $B \to A$: $\{\{\{inf_B\}_{k_B}, \omega(k_B)\}_{SK_B}\}_{PK_A}$.
(4) $A \to B$: $\{\{\omega(k_B), k_A\}_{SK_A}\}_{PK_B}$.

The following assumptions are obvious and reasonable in the rational exchange protocol.

$$A \mid\equiv \overset{SK_B}{\longmapsto} B$$

$$A \mid\equiv \overset{SK_A}{\longmapsto} A$$

$$A \mid\equiv \overset{PK_B}{\longmapsto} B$$

$$A \mid\equiv \overset{PK_A}{\longmapsto} A$$

$$A \mid\equiv \overset{PK_B}{\longmapsto} A$$

$$A \mid\equiv \overset{PK_A}{\longmapsto} B$$

$$A \mid\equiv \overset{k_A}{\longmapsto} A$$

$$A \mid\equiv \left(B \Longmapsto \{inf_B\}_{k_B}\right)$$

$$A \mid\equiv \#\{inf_B\}_{k_B}$$

$$B \mid\equiv \overset{SK_B}{\longmapsto} B$$

$$B \mid\equiv \overset{SK_A}{\longmapsto} A$$

$$B \mid\equiv \overset{PK_B}{\longmapsto} B$$

$$B \mid\equiv \overset{PK_A}{\longmapsto} A$$

$$B \mid\equiv \overset{PK_B}{\longmapsto} A$$

$$B \mid\equiv \overset{PK_A}{\longmapsto} B$$

$$B \mid\equiv \overset{k_B}{\longmapsto} B$$

$$B \mid\equiv \left(A \Longmapsto \{inf_A\}_{k_A}\right)$$

$$B \mid\equiv \#\omega\left(k_B\right)$$
$$B \mid\equiv \#\left\{inf_A\right\}_{k_A}. \tag{2}$$

Theorem 4 (security). *Under specific assumptions listed above, the presented rational exchange protocol is secure under BAN logic. Specifically, there are four potential objectives: ① $A \mid\equiv \{inf_B\}_{k_B}$; ② $B \mid\equiv \{inf_A\}_{k_A}$; ③ $A \mid\equiv \omega(k_B)$; and ④ $B \lhd k_A$.*

If the protocol is secure under BAN logic, when the protocol is completely finished, all objectives are concluded. Additionally, after Step (2), objective ② is concluded. Furthermore, after Step (3), objectives ① and ③ are additively concluded.

Proof of Theorem 4. For Step (2),

$$\frac{B \lhd \left\{\left\{\left\{inf_A\right\}_{k_A}\right\}_{SK_A}\right\}_{PK_B}, B \mid\equiv\overset{SK_B}{\longmapsto} B}{B \lhd \left\{\left\{inf_A\right\}_{k_A}\right\}_{SK_A}}$$

$$\frac{B \lhd \left\{\left\{inf_A\right\}_{k_A}\right\}_{SK_A}, B \mid\equiv\overset{PK_A}{\longmapsto} B}{B \lhd \left\{inf_A\right\}_{k_A}}$$

$$\frac{B \lhd \left\{inf_A\right\}_{k_A}, B \mid\equiv\overset{k_A}{\longmapsto} A}{B \mid\equiv A \mid\sim \left\{inf_A\right\}_{k_A}} \tag{3}$$

$$\frac{B \mid\equiv A \mid\sim \left\{inf_A\right\}_{k_A}, B \mid\equiv \#\left\{inf_A\right\}_{k_A}}{B \mid\equiv A \mid\equiv \left\{inf_A\right\}_{k_A}}$$

$$\frac{B \mid\equiv A \mid\equiv \left\{inf_A\right\}_{k_A}, B \mid\equiv \left(A \longmapsto \left\{inf_A\right\}_{k_A}\right)}{B \mid\equiv \left\{inf_A\right\}_{k_A}}$$

For Step (3),

$$\frac{A \lhd \left\{\left\{\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right\}_{SK_B}\right\}_{PK_A}, A \mid\equiv\overset{SK_A}{\longmapsto} A}{A \lhd \left\{\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right\}_{SK_B}}$$

$$\frac{A \lhd \left\{\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right\}_{SK_B}, A \mid\equiv\overset{PK_B}{\longmapsto} A}{A \lhd \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}$$

$$\frac{A \lhd \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right), A \mid\equiv\overset{k_B}{\longmapsto} B}{A \mid\equiv B \mid\sim \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}$$

$$\frac{A \mid\equiv \#\left\{inf_B\right\}_{k_B}}{A \mid\equiv \#\left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}$$

$$\frac{A \mid\equiv B \mid\sim \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right), A \mid\equiv \#\left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}{A \mid\equiv B \mid\equiv \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}$$

$$\frac{A \mid\equiv B \mid\equiv \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right), A \mid\equiv \left(B \longmapsto \left\{inf_B\right\}_{k_B}\right)}{A \mid\equiv \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}$$

$$\frac{A \mid\equiv \left(\left\{inf_B\right\}_{k_B}, \omega\left(k_B\right)\right)}{A \mid\equiv \left\{inf_B\right\}_{k_B}, A \mid\equiv \omega\left(k_B\right)} \tag{4}$$

For Step (4),

$$\frac{B \lhd \left\{\left\{\omega\left(k_B\right), k_A\right\}_{SK_A}\right\}_{PK_B}, B \mid\equiv\overset{SK_B}{\longmapsto} B}{B \lhd \left\{\omega\left(k_B\right), k_A\right\}_{SK_A}}$$

$$\frac{B \lhd \left\{\omega\left(k_B\right), k_A\right\}_{SK_A}, B \mid\equiv\overset{PK_A}{\longmapsto} B}{B \lhd \left(\omega\left(k_B\right), k_A\right)} \tag{5}$$

$$\frac{B \lhd \left(\omega\left(k_B\right), k_A\right)}{B \lhd \omega\left(k_B\right), B \lhd k_A}$$

□

Fairness. When the protocol is finished, participant's utility consists of two parts. The first part comes from the exchanged information. Let U^+ and U^- be positive and negative utility, respectively. There is an assumption, in the protocol, that both inf_A and inf_B are equal-value. It means that both $U^+(inf_B) = U^+(inf_A)$ and $U^-(inf_A) = U^-(inf_B)$ hold. Hence, after exchanging information, P_A's total utility is $U^+(inf_B) + U^-(inf_A) = 0$ and P_B's total utility is $U^+(inf_A) + U^-(inf_B) = 0$.

The remainder part is the utility derived from the contribution value. Here, participant P_i's utility is $U_i = -c_i T_i + H_i(\sum_{j=1}^{n} w_{ij} + Z_i)T_i$. In this protocol, w_{AB} is P_B's credit on P_A's QoS. In a single interaction between P_A and P_B, for participant P_A, the larger w_{AB} is, the larger U_A is. Hence, P_A will positively promote QoS. Certainly, the larger Z_A is, the larger U_A is. Here, Z_A is the reference level for other participants that interacts with P_A in future. Obviously, payments are proportional to utility for all participants. Hence, the presented rational exchange protocol is rationally fair. The quantitative analysis of fairness is elaborated in Section 5.

In a word, in the proposed rational exchange protocol, participants positively participate in executing the protocol. In such a way, all participants can obtain maximum expected utility. Hence, the protocol satisfies fairness.

Robustness. In the presented rational exchange protocol in Section 4.1, only Steps (2), (3), and (4) may suffer destabilization or interruption.

(i) In Step (2), participant P_A can abort the protocol by sending nothing. In such a case, P_B receives nothing and will not be executing the following steps. So, the utility for P_A and P_B is 0. The fairness is satisfied.

(ii) In Step (3), after receiving m_1 sent by P_A, P_B can interrupt the protocol by not sending m_2. Now, P_B can

Table 2: Theoretical comparisons between rational exchange protocols.

Scheme	Information type	With entropy	Quantification of utility	Rational fairness
Syverson's [9]	Complete	✘	✘	✘
Buttyán's [10]	Complete	✘	✘	✘
Alcaide's [11]	Imperfect[1]	✘	✘	✔
Alcaide's [12]	Complete	✘	✘	✔
Ours	Asymmetric	✔	✔	✔

[1]Imperfect information is not suitable for realistic application scenarios.

not derive inf_A since the unawareness of k_A. Hence, P_B still knows nothing about inf_A and the protocol is still fair.

(iii) In Step (4), P_A can interrupt the protocol by not sending m_3 after receiving m_2 sent by P_B. In such a case, P_B can make an argument on this exchange, and *PUB* will mark inf_B invalid and rate a negative feedback for P_A according to the QoS evaluation mechanism proposed in Section 3.2. The negative feedback lowers Z_A and is a severe punishment for P_A. Simultaneously, P_B will also rate a low w_{AB}. Hence, P_A's utility $U_A = -c_A T_A + H_A(\sum_{j=1}^{n} w_{Aj} + \ln Z_A)T_A$ is inevitable lower than that before the exchange. Obviously, for long-term utility, P_A will never destabilize the protocol to maximize his own utility. Hence, the protocol is still fair.

In Steps (1) and (5), there is, obviously, no potential destabilization or interruption. Hence, in a word, the presented protocol is fair when destabilization or interruption occurs.

4.3. Theoretical Comparisons. Rational exchange protocol is a fresh and crucial branch in cryptographic research field. The greatest difference between our protocol and other related works is that related works have been investigated under complete (symmetric) information, while our protocol is very under asymmetric information. Theoretical comparisons are legibly declared in Table 2.

In rational exchange protocol, complete information is an ideal assumption which violates the requirements in realistic environment. Rational exchange protocol under imperfect information is first investigated in Alcaide's protocol [11]. The complete but imperfect information in [11] is, however, not suitable for the scenarios in Section 1. In this paper, rational exchange protocol under asymmetric information is carefully designed with clear definition and much more compatible for practice.

It is striking that the utility in existing rational exchange protocol can not be quantized so far, since the absence of entropy. Information theory is introduced in this paper to quantize all participants' utilities. Such a way is the first attempt to clearly evaluate participant's utility. Participant can further make accurate decisions by observing participants' utilities. Obviously, such a characteristic is more compatible and operable for real applications.

Rational fairness is an important characteristic for rational exchange protocol and has been attracting vastly attention in cryptographic community. Through analysis under a dynamic model with entropy in Section 4.2, rational fairness is guaranteed.

5. Simulation of Utility Function with Entropy

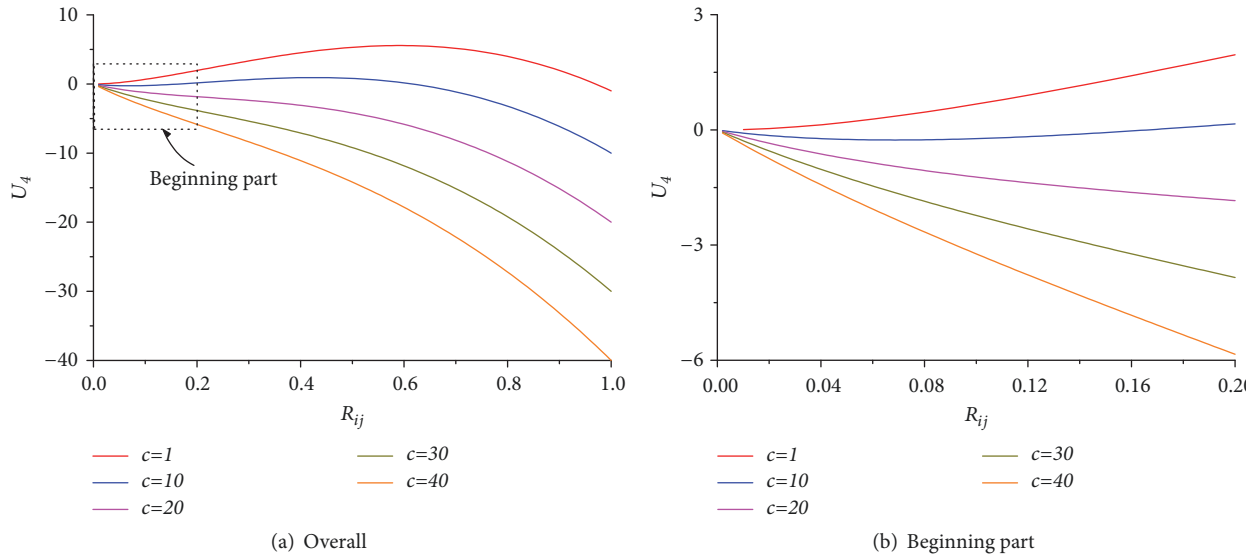
The utility function with entropy is kernel to guarantee the fairness of rational exchange protocol. In this section, through simulation, the proposed utility function with entropy is investigated in detail.

5.1. Simulation Environment. In the following simulation, the number of participants is assumed to be 10. When the system achieves stabilization after several rounds of information exchange, the current transfer matrix $\mathtt{P}$ of participants' types for each participant is assumed same and given as follows.

$$\mathtt{P} = \begin{bmatrix} 0.8 & 0.2 & 0 & 0 \\ 0.2 & 0.6 & 0.2 & 0 \\ 0 & 0.3 & 0.5 & 0.2 \\ 0 & 0 & 0.3 & 0.7 \end{bmatrix} \tag{6}$$

By resolving a system of linear equations $\mathtt{D} = \mathtt{D} \bullet \mathtt{P}$, the steady-state vector is $\mathtt{D} = \{0.32, 0.32, 0.22, 0.14\}$. The vector containing all membership functions is given as $\mathtt{g} = \{1.0, 0.75, 0.5, 0\}$, in which great $\mathtt{g}_i$ (i.e., closer to 1) indicates high-level accuracy of $\mathtt{D}_i$. Then, the probability of participant P_j serving P_i is $R_{ij} = \mathtt{D} \bullet \mathtt{g}^T = 0.67$. To evaluate participant's credits on the process of information exchange, all the vectors $(w_{ij})_{P_j \in \mathbb{P} \setminus \{P_i\}}$ of credits for participant P_i are generated randomly such that $w_{ij} \in (0, 1)$ and $w_{ii} = 0$. In a similar way, the vector Z_i of positive feedbacks is calculated through the above probabilities for all participants in the protocol.

The contribution value for participant P_i is $T_i = \alpha \sum_{j=1}^{n} R_{ij}$, in which $\alpha \in (0, 1)$. Here, let $\alpha = 0.1$, and $T_i = 0.1 \times (10 - 1) \times 0.67 = 0.603$ and $H_i = -\sum_{j=1}^{n} R_{ij} \ln R_{ij} = 2.41$ are derived. Given a unitary cost, the utility for each participant can be derived. All the values calculated in the above equations are listed below.



(a) Overall (b) Beginning part

FIGURE 4: The effectiveness on utility function while varying c_4 with $\alpha = 0.1$ for participant P_4.

The matrix W of credits is generated in the following.

$$\begin{bmatrix} 0.00 & 0.43 & 0.85 & 0.42 & 0.78 & 0.23 & 0.55 & 0.93 & 0.64 & 0.21 \\ 0.96 & 0.00 & 0.62 & 0.05 & 0.39 & 0.35 & 0.30 & 0.78 & 0.38 & 0.30 \\ 0.00 & 0.18 & 0.00 & 0.90 & 0.24 & 0.82 & 0.74 & 0.49 & 0.81 & 0.47 \\ \underline{0.77} & \underline{0.26} & \underline{0.51} & \underline{0.00} & \underline{0.40} & \underline{0.02} & \underline{0.19} & \underline{0.44} & \underline{0.53} & \underline{0.23} \\ \mathbf{0.79} & \mathbf{0.98} & \mathbf{0.83} & \mathbf{0.76} & \mathbf{0.00} & \mathbf{0.99} & \mathbf{0.83} & \mathbf{0.73} & \mathbf{0.78} & \mathbf{0.82} \\ 0.87 & 0.14 & 0.08 & 0.49 & 0.13 & 0.00 & 0.18 & 0.31 & 0.94 & 0.19 \\ 0.08 & 0.87 & 0.24 & 0.34 & 0.94 & 0.65 & 0.00 & 0.51 & 0.88 & 0.23 \\ 0.40 & 0.58 & 0.12 & 0.90 & 0.96 & 0.73 & 0.63 & 0.00 & 0.55 & 0.17 \\ 0.26 & 0.55 & 0.18 & 0.37 & 0.58 & 0.65 & 0.78 & 0.82 & 0.00 & 0.23 \\ 0.80 & 0.14 & 0.24 & 0.11 & 0.06 & 0.45 & 0.08 & 0.79 & 0.59 & 0.00 \end{bmatrix} \quad (7)$$

Assume that participant will respond to a positive feedback when the credit is greater than 0.60. Obliviously, the vector Z of positive feedbacks is simulated in the following.

$$Z = (4, 3, 4, \underline{1}, \mathbf{9}, 2, 4, 4, 3, 2). \quad (8)$$

The utility U for all participants is calculated in the following.

$$(9.28, 7.54, 8.71, \underline{4.81}, \mathbf{14.05}, 5.79, 8.84, 9.28, 7.96, 5.68). \quad (9)$$

By observing the utilities for all participants, participant P_5's utility is maximal and participant P_4's utility is minimal. It is consistent with the generated credits that P_5's credits are significantly greater than other participant's and P_4's credits are significantly smaller than other participant's. Hence, the presented utility function with entropy appropriately reflects the realistic utilities for all participants.

5.2. Effect of Parameters. The utility function with entropy $U_i = -c_i T_i + H_i(\sum_{j=1}^{n} w_{ij} + \ln Z_i)T_i$ is thoroughly investigated by observing P_4 and P_5's utilities by varying c and α, respectively.

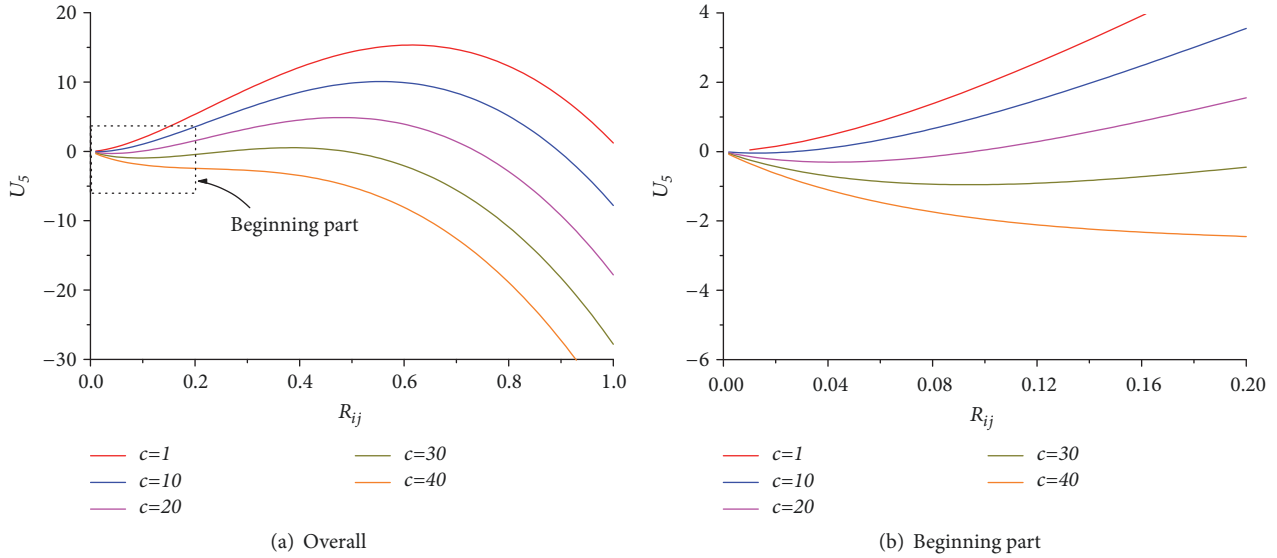
Effect of c. We vary $c \in \{1, 10, 20, 30, 40\}$ to exhibit the effectiveness on the presented utility function. The simulation is illustrated in Figures 4 and 5. Specifically, in Figure 4, Figure 4(b) illustrates the particulars of utility U_4's beginning tendency for participant P_4. In a similar way, Figure 5(b) illustrates the details of P_5's utility that is depicted in dotted rectangle in Figure 5(a). It is striking that participant's utility decreases at the beginning, increases in the middle stage, and decreases again at the end. In general, participant P_i's utility U_i is acquired in exchange with other participants. The trends of utility function confirm real-world scenarios and are elaborately described in the following content.

At the very beginning, participant P_j is considered to be outside indeed. Participant P_i's utility coming from P_j is assumed to be 0. During the first increasing of participant P_j's service probability, R_{ij} is extremely small and less than a threshold. Although the probability increases, the incrementation does not put any positive effect on U_i. P_i still, however, pays out due to the participation in the exchange. The utility coming from such an incrementation does not counteract the payment. Hence, U_i decreases in such a stage.

In the next stage, with the incrementation of P_j's service probability, the utility coming from such an incrementation goes beyond the payment. Hence, U_i increases along with the increasing of probability. Such a situation is compatible for practice and provides a guarantee of fairness for all participants.

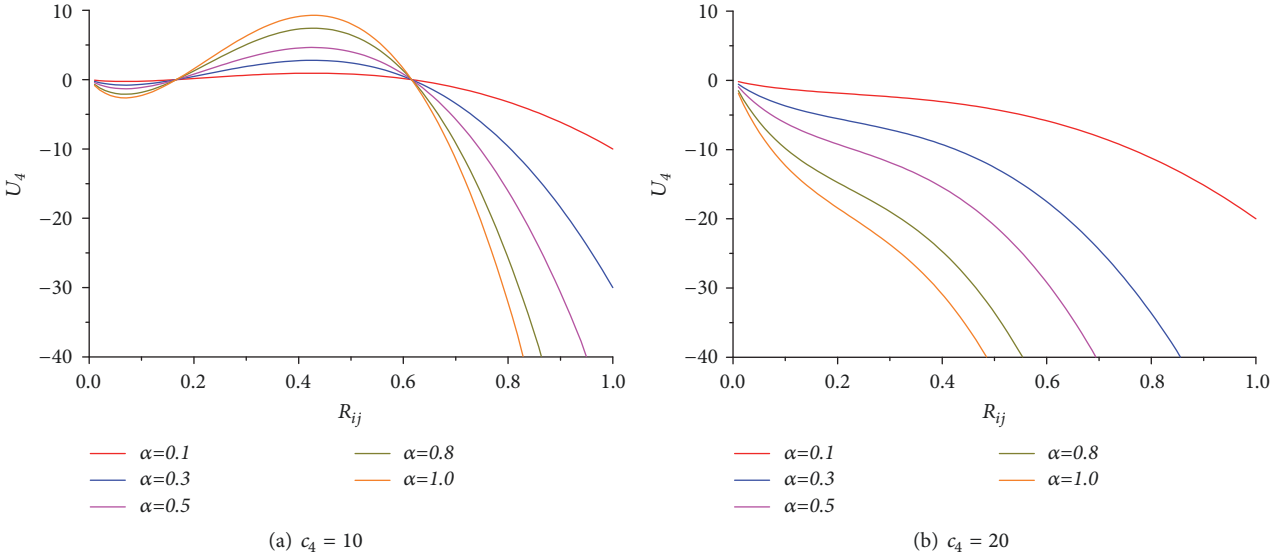
In the ending stage, if P_j's service probability is close to 1, other participants will free ride potentially. Due to that, participant P_i's credits and positive feedbacks will decrease. Following that, the utility U_i inevitably decreases in future. That is still fair for all participants.

Effect of α. We vary $\alpha \in \{0.1, 0.3, 0.5, 0.8, 1.0\}$ to exhibit the effectiveness on utility function. The simulation is illustrated in Figures 6 and 7. It is striking that the utility's tendency



(a) Overall (b) Beginning part

Figure 5: The effectiveness on utility function while varying c_5 with $\alpha = 0.1$ for participant P_5.



(a) $c_4 = 10$ (b) $c_4 = 20$

Figure 6: The effectiveness on utility function while varying α with $c_4 = 10$ and $c_4 = 20$ for participant P_4.

is consistent with that while varying c. Additionally, with greater α, the utility's discrimination is more prominent. In practice, α is determined according to consumer's realistic requirements.

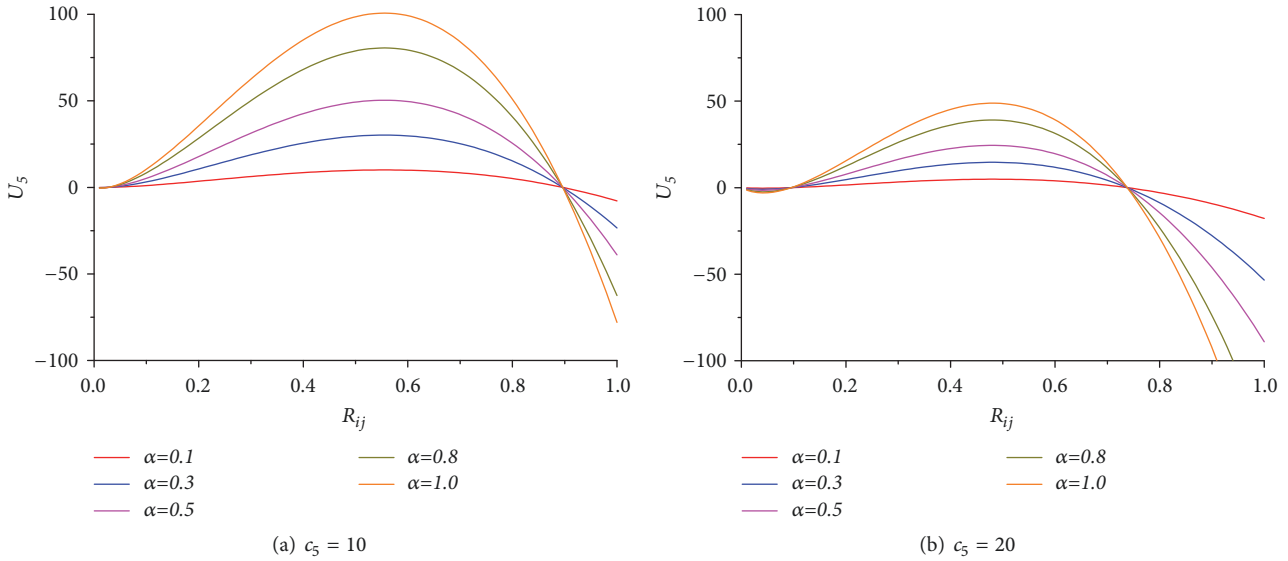
5.3. Performance for Participants. In this section, performance for all participants is elaborated in detail by varying contribution weight α and unitary cost c, respectively.

Varyingα. In the evaluation of performance, contribution weight α is varied in $(0.0, 1.0)$ in Figure 8(a). Obviously, with the increment of α, the discrimination between utilities for all participants is increasing significantly. The significant discrimination is important for practice, due to the fact that participant can facilely make decision without any doubt.

Wallrabenstein 2014 Varying c. In the evaluation of performance, contribution weight c is varied in $(0, 40)$ in Figure 8(b). Obviously, with the increment of α, the discrimination between utilities for all participants remains the same, due to the fact that a theoretical assumption that the probability of participant P_j serving P_i is R_{ij} is the same for all participants. Although the probabilities are completely different in practice, the discrimination remains the same since that the change of c only lowers the coefficient of T_i and does not change the monotonicity of utility in (1).

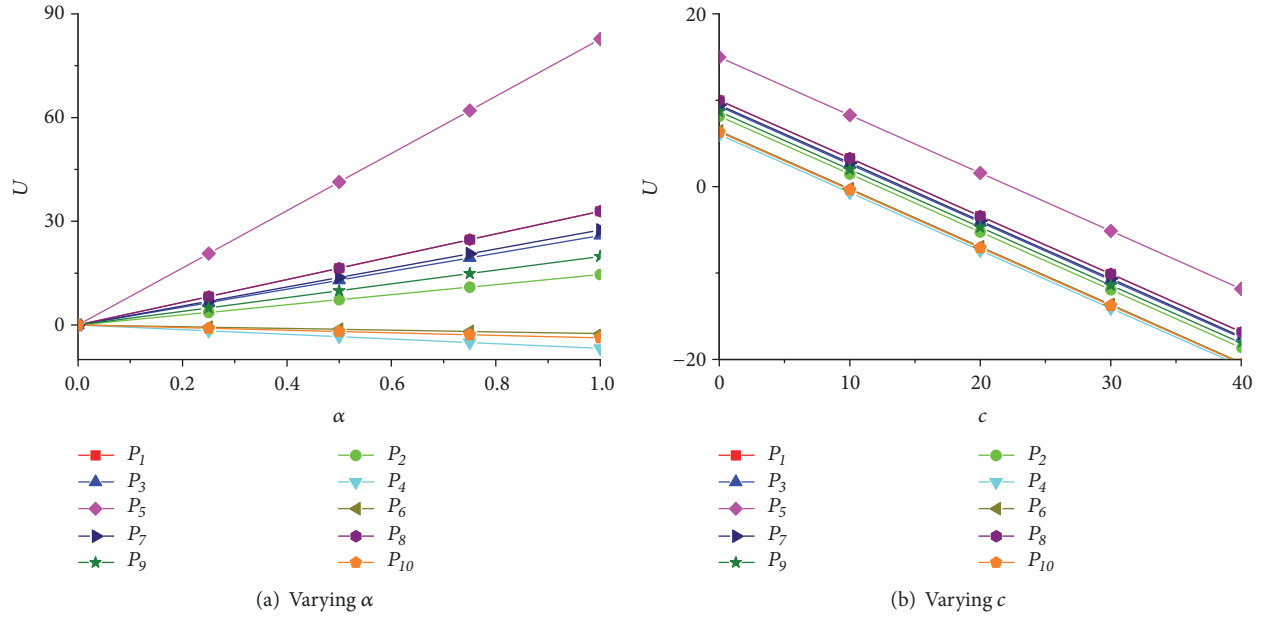
6. Related Work

Cryptography and game theory both concentrate on designing protocol, in which participants are with potential conflicts



(a) $c_5 = 10$ (b) $c_5 = 20$

FIGURE 7: The effectiveness on utility function while varying α with $c_5 = 10$ and $c_5 = 20$ for participant P_5.



(a) Varying α (b) Varying c

FIGURE 8: The performance of utility function with entropy for all participants. In Figure 8(a), α is varied with $c = 10$ and in Figure 8(b) c is varied with $\alpha = 0.1$.

of benefits [17, 18]. By combining both theories, rational secret sharing and rational secure multiparty computation are proposed by Halpern et al. [5] in 2004. In traditional cryptography, participants are assumed to be honest (strictly follow the protocol) or malicious (violate or destroy the protocol), and participants are however rational instead in practice for WSNs. That means all participants are highly willing to maximize their utilities by selecting their strategies during the whole protocol. That brings enormous challenge in designing protocols. Since the proposal of rational cryptography, there exist a number of studies [19, 20], such as rational secret sharing [21] and rational secure multiparty computation [5]. Indeed, rational exchange protocol, which guarantees security and fairness for peers in WSNs, is practical and necessary for realistic environments.

In 1998, Asokan [22] proposed an interactive protocol to exchange digital signature in a fair manner. It is the prototype of rational exchange protocol. The first real rational exchange protocol is proposed based on a weakly secret bit commitment function by Syverson [9] in the same year. In 2001, Buttyán et al. [10] analyzed the fairness of Syverson's protocol based on game theory, and, in 2004, they modeled rational exchange protocol and further analyzed the fairness of Syverson's protocol [13]. After that, Alcaide et al. modeled

rational exchange protocol based on extended game theory and Bayesian game in [11], improved Syverson's protocol in [23], and designed rational exchange protocol based on nature-inspired synthesis [12, 14]. However, all the above rational exchange protocols are constructed in environments with complete information, which is not perfectly compatible for scenarios mentioned in Section 1.

Rational participants possess asymmetric information about each other in real-world scenarios. Rational exchange protocol in such scenarios is not well investigated so far. By further combining information theory, rational exchange protocol is more practical and compatible for WSN. So far, information theory has been introduced into several cryptographic protocols [24, 25]. However, rational exchange protocol under asymmetric information is not thoroughly studied, which is striking in this paper.

7. Conclusion

In this paper, we presented a rational exchange protocol under asymmetric information, which is compatible and practical for WSNs. First of all, a dynamic game model with entropy is presented to quantify utilities of participants. In such a game, utilities for all participants can be quantized. Following that, a utility function with entropy is designed based on integrating a Markov-based entropy function and a novel QoS evaluation model. Furthermore, the concrete rational exchange protocol is presented with thorough analysis. Finally, the utility function with entropy is simulated. The simulation demonstrates effectiveness and availability of the presented rational exchange protocol.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant nos. 61702403, 61472298, 61662009, and 61472310), the Fundamental Research Funds for the Central Universities (Grant no. JB170308), the Project funded by China Postdoctoral Science Foundation (Grant no. 2018M633473), and the National Cryptography Development Foundation of China (Grant no. MMJJ20170129).

References

[1] M. Karakaya, K. Ibrahim, and U. Özgür, "Counteracting free riding in Peer-to-Peer networks," *Computer Networks*, vol. 52, no. 3, pp. 675–694, 2008.

[2] M. Karakaya, I. Korpeoglu, and Ö. Ulusoy, "Free riding in peer-to-peer networks," *IEEE Internet Computing*, vol. 13, no. 2, pp. 92–98, 2009.

[3] F. Malandrino, C. Casetti, and C.-F. Chiasserini, "Discovery and provision of content in vehicular networks," *Wireless Communications and Mobile Computing*, vol. 13, no. 3, pp. 244–254, 2013.

[4] H. Li, X. Liu, W. He, W. Yang, and W. Dou, "Delay analysis in practical wireless network coding," *Wireless Communications and Mobile Computing*, vol. 14, no. 5, pp. 497–515, 2014.

[5] J. Halpern and V. Teague, "Rational secret sharing and multiparty computation: extended abstract," in *Proceedings of the 36th Annual ACM Symposium on Theory of Computing (STOC 04)*, pp. 623–632, New York, NY, USA, 2004.

[6] G. Fuchsbauer, J. Katz, and D. Naccache, "Efficient rational secret sharing in standard communication networks," in *Theory of Cryptography*, D. Micciancio, Ed., pp. 419–436, Springer, Berlin, Germany, 2010.

[7] J. Garay, J. Katz, U. Maurer, B. Tackmann, and V. Zikas, "Rational protocol design: Cryptography against incentive-driven adversaries," in *Annual Symposium on Foundations of Computer SCIence—FOCS*, pp. 648–657, 2013.

[8] X. Liu, R. Deng, K. R. Choo, Y. Yang, and H. Pang, "Privacy-Preserving Outsourced Calculation Toolkit in the Cloud," *IEEE Transactions on Dependable and Secure Computing*, 2018.

[9] P. Syverson, "Weakly secret bit commitment: applications to lotteries and fair exchange," in *Proceedings of the 11th IEEE Computer Security Foundations Workshop*, pp. 2–13, Rockport, MA, USA.

[10] L. Buttyán and H. Jean-Pierre, "Rational Exchange - A Formal Model Based on Game Theory," in *Electronic Commerce*, vol. 2232 of *Lecture Notes in Computer Science*, pp. 114–126, Springer Berlin Heidelberg, Berlin, Germany, 2001.

[11] A. Alcaide, J. M. Estevez-Tapiador, J. C. Hernandez-Castro, and A. Ribagorda, "An Extended Model of Rational Exchange Based on Dynamic Games of Imperfect Information," in *Emerging Trends in Information and Communication Security*, G. Müller, Ed., pp. 396–408, Springer, Berlin, Germany, 2006.

[12] A. Alcaide, J. M. Tapiador, J. C. Hernandez-Castro, and A. Ribagorda, "Nature–Inspired Synthesis of Rational Protocols," in *Parallel Problem Solving from Nature – PPSN X*, G. Rudolph, T. Jansen, N. Beume, S. Lucas, and C. Poloni, Eds., pp. 981–990, Springer, Berlin, Germany, 2008.

[13] L. Buttyán, J. Hubaux, S. Capkun, and S. Schneider, "A formal model of rational exchange and its application to the analysis of Syverson's protocol," *Journal of Computer Security*, vol. 12, no. 3-4, pp. 551–587, 2004.

[14] A. Alcaide, J. Estevez-Tapiador, J. Hernandez-Castro, and A. Ribagorda, "A multi-party rational exchange protocol," in *On the Move to Meaningful Internet Systems 2007:OTM2007 Workshops, ser. Lecture Notes in Computer Science*, R. Meersman, Z. Tari, and P. Herrero, Eds., vol. 4805, pp. 42-43, Springer, Berlin, Germany, 2007.

[15] S. Lauermann, "Asymmetric information in bilateral trade and in markets: an inversion result," *Journal of Economic Theory*, vol. 147, no. 5, pp. 1969–1997, 2012.

[16] M. Burrows, M. Abad, and M. Needham, "A logic of authentication," *The Royal Society A Mathematical, Physical and Engineering Sciences*, vol. 426, no. 1871, pp. 233–271, 1989.

[17] P. Li, J. Li, Z. Huang et al., "Multi-key privacy-preserving deep learning in cloud computing," *Future Generation Computer Systems*, vol. 74, pp. 76–85, 2017.

[18] J. Li, X. Chen, S. S. Chow, Q. Huang, D. S. Wong, and Z. Liu, "Multi-authority fine-grained access control with accountability and its application in cloud," *Journal of Network and Computer Applications*, vol. 112, pp. 89–96, 2018.

[19] J. Alwen, C. Cachin, J. B. Nielsen et al., "Summary report on rational cryptographic protocols," University of Aarhus, 2007.

[20] Z. Zhang and M. Liu, "Rational secret sharing as extensive games," *Science China Information Sciences*, vol. 56, no. 3, 032107, 13 pages, 2013.

[21] W. K. Moses and C. P. Rangan, "Rational secret sharing over an asynchronous broadcast channel with information theoretic security," *International Journal of Network Security and Its Applications*, vol. 3, no. 6, pp. 1–18, 2011.

[22] N. Asokan, *Fairness in electronic commerce [Ph.D. thesis]*, University of Waterloo, 1998.

[23] A. Alcaide, E.-T. U. M, H.-C. J. C, and A. Ribagorda, "Cryptanalysis of syversons rational exchange protocol," *International Journal of Network Security*, vol. 7, no. 2, pp. 151–156, 2008.

[24] U. Maurer, "Information-theoretically secure secret-key agreement by NOT authenticated public discussion," in *Advances in cryptology-EUROCRYPT '97 (Konstanz)*, W. Fumy, Ed., vol. 1233, pp. 209–225, Springer, Berlin, Germany, 1997.

[25] R. Renner and S. Wolf, "The exact price for unconditionally secure asymmetric cryptography," in *Advances in Cryptology-EUROCRYPT 2004*, C. Cachin and and J. L. Camenisch, Eds., pp. 109–125, Springer, Berlin, Germany, 2004.