EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Security and quality of service (QoS) co-design in cooperative mobile *ad hoc* networks

F Richard Yu[1*], Helen Tang[2], Shengrong Bu[1] and Du Zheng[1]

Abstract

Cooperative communication has been considered as a promising technique to improve communication quality of service (QoS) in wireless networks, including mobile *ad hoc* networks (MANETs). Due to their unorganized and decentralized infrastructure, cooperative MANETs (CO-MANETs) are vulnerable to attacks initiated on relays. Although encryption and authentication protocols may prevent compromised data transmission when a selected relay is attacked, their cost is high. In this paper, we propose a game-theoretic approach to quantitatively analyze the attack strategies of the attacker so as to make a rational decision on relay selection and the authentication parameter adaptation to reach a trade-off between security and QoS in CO-MANETs. Simulation results show the effectiveness of the proposed approach for security and QoS co-design in CO-MANETs.

Keywords: Security; Quality of service; Game theory; MANETs

1 Introduction

Cooperative communication has been considered as a promising technique to improve quality of service (QoS) in wireless networks through the cooperation of users. The idea behind cooperative communication is that single-antenna mobile nodes in a multiuser scenario can share their antennas in a manner that creates a virtual multiple-input and multiple-output (MIMO) system [1]. Transmitting independent copies of the signal generates diversity and can effectively combat the deleterious effects of fading. Particularly, selecting the most suitable relay among available relays can achieve selection diversity in cooperative communications [2-4]. This promising technique has been considered in the IEEE 802.16j standard and is expected to be integrated into future 3GPP cellular networks [5].

While cooperative communication brings significant benefits, it also raises serious security issues. Particularly, mobile *ad hoc* networks (MANETs) with cooperative communications (CO-MANETs) [6] present significant challenges to secure routing, key exchange, key distribution and management, as well as intrusion detection and protection. For example, it is possible for malicious nodes to join the network and relay unsolicited information to a rogue destination, thereby compromise the network. It is also possible for some nodes to act in a selfish manner to conserve their own energy and not cooperate and relay information from other nodes, thereby discouraging cooperation.

Although encryption and authentication protocols can prevent compromised data transmission when the selected relay is attacked, these measures consume scarce bandwidth and reduce system throughput. It would be desirable to choose only trustworthy nodes as relays and only authenticate the packets through the nodes that are prone to attack. To achieve this goal, we would need to design a quantitative approach to analyze the actions of the attackers so as to make appropriate decisions on relay selection and the extent that encryption and authentication protocols are required.

Game-theoretic approaches have been proposed to improve network security [7]. Game theory addresses problems in which multiple players with contradictory incentives or goals compete with each other; thus, it can provide a mathematical framework for modeling and analyzing decision problems. In game theory, one player's outcome depends not only on her/his decisions, but also on those of her/his opponents' decisions. Similarly, the success of a security scheme depends not only on the

*Correspondence: richard_yu@carleton.ca
[1] Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada
Full list of author information is available at the end of the article

actual defense strategies, but also on the actions taken by the attackers.

In this paper, we propose a quantitative decision-making approach that is based on game theory and takes both security and QoS in terms of throughput into consideration. To the best of our knowledge, using a game theoretical approach to jointly study security and QoS issues for MANETs with cooperative communications has not been considered in existing works. We propose a dynamic Bayesian game-theoretic approach to enable a node to make strategic decisions on relay selection and authentication parameter adaptation. A Bayesian game is a game in which the information about the characteristics of other players is incomplete [8]. A node in the network can update its beliefs in the maliciousness of relays according to the record of attack history. It does not need to authenticate all packets because there exists a possibility that the selected relay will not be attacked by the attacker. Compared with the approach proposed in [9] that authenticates all the packets without considering the possibility that the selected relay is cooperative, the proposed game-theoretic approach only authenticates the packets through the nodes prone to attack. Therefore, the proposed scheme can avoid unnecessary consumption of system resources and leads to a better system performance in terms of system throughput, which is shown in the simulation results.

We use an adaptive and lightweight protocol for both hop-by-hop and end-to-end authentications (ALPHA) [10], which is based on hash chains and Merkle trees, i.e., a tree of hashes. We take an integrated design approach to optimize the number of messages (or leaves) in the Merkle tree (an important parameter in the authentication scheme) and relay selection (an important process for QoS provisioning in cooperative communication networks). We will show that security schemes have significant impacts on the QoS in terms of throughput of MANETs, and our proposed scheme can improve the system throughput of MANETs with cooperative communications compared to the existing approach [7] that authenticates all packets.

The rest of the paper is organized as follows. Section 2 presents the related work. The proposed game-theoretic approach is presented in Section 3. Simulation results and discussions are given in Section 4. Finally, we conclude this paper in Section 5.

2 Related work

2.1 Cooperative communication

Cooperative communication allows single-antenna mobiles to reap some of the benefits of MIMO systems. The fundamental idea behind cooperative communication is that single-antenna mobiles in a multiuser scenario can share their antennas in a manner that creates a virtual MIMO system. It is well-known that the mobile wireless channel suffers from fading; in another word, signal attenuation can vary significantly over the course of a given transmission. Transmitting independent copies of the signal generates diversity and can effectively combat the deleterious effects of fading. Particularly, spatial diversity is generated by transmitting signals from different locations, thus allowing independently faded versions of the signal to arrive at the receiver [11,12]. Cooperative communication generates spatial diversity in a new and interesting way. As illustrated in Figure 1, in which a node represents a mobile device with one antenna, two nodes are communicating with the same destination. Each node has one antenna and cannot individually realize spatial diversity. However, it is possible for one node to receive the information sent from the other, in which case, it could forward received information along with its own information to the destination. Since the fading path from two nodes is statistically independent, spatial diversity is achieved [13].

In this study, we consider the mobile ad hoc networks, in which users may increase their effective quality of services through cooperation. Each wireless user is assumed to transmit data as well as function as cooperative relay to forward received data from its partners.

2.2 Opportunistic relaying

The proposed game-theoretic approach in this paper adopts a proactive opportunistic relaying process. As the name implies, opportunistic relaying selects the best relay according to different relay selection criteria among all candidate relays to forward the signal between the source and the destination [14]. An opportunistic relaying process consists of two time slots. In the first time slot, the source broadcasts the signal which could be heard by all

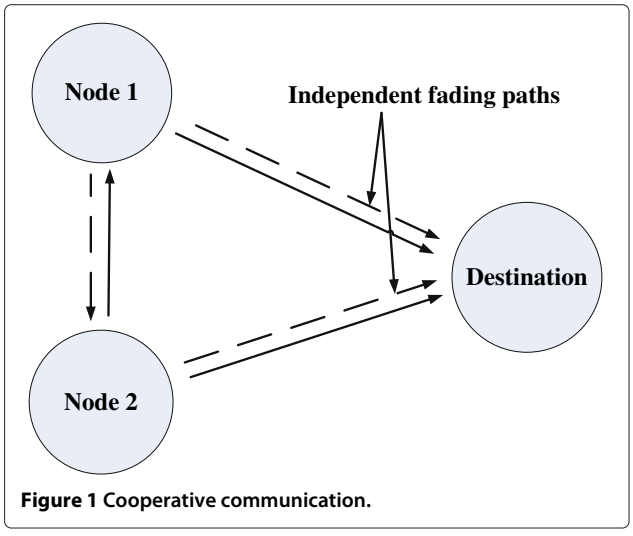

Figure 1 Cooperative communication.

relay nodes in its radio coverage and the destination; in the second time slot, if the signal received by the selected relay node could be decoded successfully, it would be forwarded to the destination; the destination then combines the received signal from the source and selected relay to recover the information sent from the source. The source selects the best relay before transmitting the data from the source to the destination [15]. There is no requirement on all intermediate relays to listen to the source's broadcasting except for the selected relay; thus, power or energy spent by unselected relays on listening to the channel and receiving the message sent by the source is saved. There are three proactive diversity schemes: fixed selective decode-and-forward (FSDF) with direct link combining, FSDF without direct link combining, and smart selective decode-and-forward [16].

2.3 Security in cooperative wireless communication networks

It is evident that cooperative communication brings significant benefit in improving the communication quality of wireless communication networks. Cooperative wireless communication was originally designed with the assumption that all the nodes involved always help each other and cooperate in a socially efficient manner. However, assumption on complete cooperation is broken by the facts that there exist relays that are attacked by the network attackers and misbehave for selfish or malicious intentions.

Thus, it is acknowledged that security is one of the main concerns for cooperative communication. Various security issues show the importance of data integrity checking and the need to have recognized reliable relationship amongst the different nodes in cooperative wireless communication networks. Authentication is a process that involves in a communication process between an *authenticator* and *supplicant* to identify the identity of the supplicant [17-19]. Sometimes a trusted third party might be involved in an authentication process. Therefore, authentication is important, with the consequent need to know exactly who we are talking to and make sure that the message received from a node is exactly the message that had been sent by that node. Authentication, therefore, supports privacy, confidentiality, and access control by verifying and validating the received message. All nodes in the cooperative wireless communication networks should be able to carry out the authentication and act as authenticator and supplicant from time to time.

The authors of [20] make a survey that focuses on node-to-node authentication for wireless communication networks and classifies authentication taxonomy based on the type of credentials. Credentials can be classified into two classes: identity-based and context-based. Identity-based credentials can be further classified into encryption-based and non-encryption-based.

For non-encryption based identity credential, information is hashed using a one-way hash function and the key processed by the supplicant. Thus, this method is computationally efficient. To verify the supplicant's identity, the authenticator must own the key used by the supplicant and know the one-way hash function used by the supplicant to regenerate the results that were disclosed by the supplicant as identity. Another form of hash based non-encryption identity credential uses a delayed key disclosure as in timed efficient stream loss-tolerant authentication (TESLA) [21], lightweight hop-by-hop authentication protocol (LHAP) [22], hop-by-hop efficient authentication protocol (HEAP) [23], and adaptive and lightweight protocol for hop-by-hop authentication (ALPHA) [10]. TESLA is a broadcast authentication protocol based on loose time synchronization. However, hop-by-hop authentication is not supported by TESLA. What is more, the computational overhead of TESLA is also high due to the existence of network latencies and redundant hash elements. LHAP bases on the principles of TESLA to carry out both packet authentication and hop-by-hop authentication, wherein intermediate nodes authenticate all the packets received prior to forwarding them. However, LHAP also suffers from long latency and poor throughput and is not designed to prevent inside attacks. HEAP authenticates packets at every hop using modified hash message authentication code-based algorithm along with two keys and dropping any packet that originates from outsiders. However, HEAP still suffers from inside attack and could not provide end-to-end authentication. ALPHA, which makes use of interaction-based hash chains and Merkle trees, provides both end-to-end and hop-by-hop authentication and integrity protection and overcomes the shortcomings of the above-proposed protocols. Therefore, ALPHA is adopted as the authentication protocol in the proposed game-theoretic approach for security and QoS co-design in cooperative wireless communication networks.

3 Proposed game-theoretic approach

In this section, the proposed game-theoretic approach for security and QoS co-design in cooperative wireless communication networks is described in detail by setting up the system model and presenting the utility of the attacker brought by attacking target selection and the utility of the source brought by relay selection, Nash equilibrium of the proposed game-theoretic approach, and equations of system performance analysis.

3.1 Model description

The proposed game-theoretic approach focuses on two-hop cooperative wireless communication networks, as

illustrated in Figure 2, consisting of source, destination, four intermediate relays, and a slow-fading channel that satisfies Rayleigh distribution. All of the relays are originally assumed to be cooperative, and the selected relay forwards the received information from the source to the destination. However, in reality, some relays are compromised by the attacker and do not do what they are supposed to do or do what they are not supposed to do.

In this paper, we represent the set of relays as $\mathcal{R}$. Attack on relays initiated by the attacker is independent from each other. The interactions between the attacker and the source are modeled as a non-cooperative game since both the tendencies of the attacker and the source are to maximize their total utility through the strategic selection of attacking target and relay. The attacker selects the attacking probability distribution $P = \{p_1, p_2, \ldots, p_K\}$ over all relays in $\mathcal{R}$, where p_i is the probability of selecting R_i as attacking target and K is the number of candidate relays in the radio coverage of the source. In each play of the game, the attacker chooses one relay to attack; thus, we have $\sum_i^K p_i = 1$. For the source, it selects all candidate relays with a probability distribution $Q = \{q_1, q_2, \ldots, q_K\}$, where q_i is the probability of selecting R_i as relay. In each play of the game, the source chooses one relay from all candidate relays; thus, we have $\sum_i^K q_i = 1$. We assume that each relay processes a combination of information and security assets denoted by $\alpha_I I_i + \alpha_S S_i$, $i \in 1, 2, \ldots, K$, which represents the loss of information and security assets when the attacker's attacking target selection coincides the source's relay selection. α_I and α_S represent the weights of information and security assets in the asset combination. The information asset of a relay depends on the mutual information, while the security asset of a relay depends on its role in the network. In practice, the information asset is evaluated by the mutual information which affects the system throughput of cooperative wireless communication networks, and the security asset is evaluated in the risk analysis using formal analysis before system deployment.

3.2 Dynamic Bayesian game-theoretic approach

The proposed dynamic Bayesian game-theoretic approach also consists of two players, the source which selects the best relay from all candidate relays that brings maximum utility and the attacker which selects relay as attacking target. The set of strategies of the source contains 'Select' and 'Not select'. 'Attack' and 'Not attack' consist of the attacker's strategies on relay R_i when the attacker may choose relay R_i to attack; otherwise, there is only one strategy when the attacker does not choose relay R_i as attacking target, i.e., Not attack. Since the source is uncertain about the type of each relay, it holds an *a priori* belief $\mu_i^{t_k}$, $i = \{1, 2, \ldots, K\}$ in the maliciousness of relay R_i at the commence of each relay selection stage t_k, $k = \{1, 2, \ldots\}$. $1 - \mu_i^{t_k}$, $i = \{1, 2, \ldots, K\}$, $k = \{1, 2, \ldots\}$, represents the source's prior belief in that relay R_i is cooperative. We assume that the game in the proposed dynamic game-theoretic approach is played repeatedly every period t_k, where $k = 0, 1 \ldots$. We assume that the utility of players in each stage remain the same. We assume that each relay node processes a combination of information and security assets denoted by $\alpha_I I_i + \alpha_S S_i$. α_I and α_S represent the weights of information and security assets in the asset combination and vary in various networks.

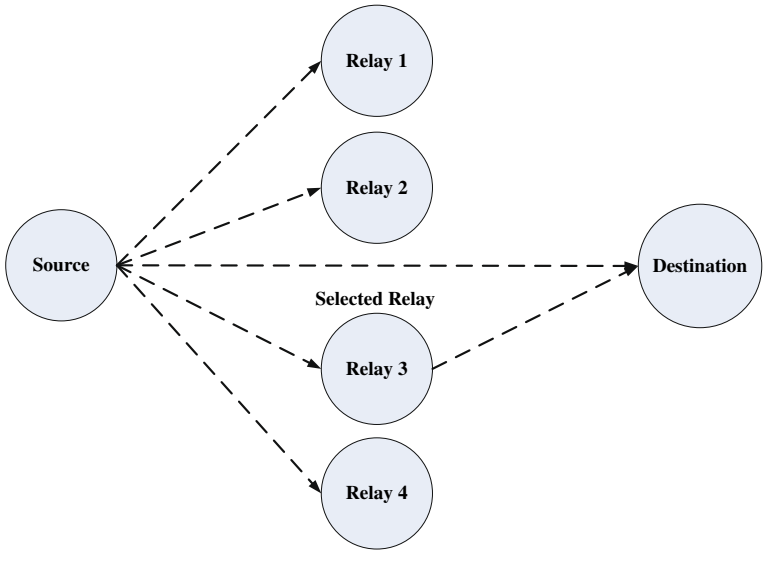

Figure 2 A cooperative wireless communication network.

If the selection of relay of the source and the selection of attacking target of the attacker coincide, the attacker will obtain utility $\alpha_I I_i + \alpha_S S_i$, while the source will lose the same amount of utility. Otherwise, the utility for the attacker and the source is $-(\alpha_I I_i + \alpha_S S_i)$ and $\alpha_I I_i + \alpha_S S_i$, respectively. Substitute $\alpha_I I_i + \alpha_S S_i$ by A_i, Table 1 illustrates the utility matrix of attacker and source on relay R_i with probability $\mu_i^{t_k}$ being malicious at stage t_k. In the matrix, a denotes the detection rate of the source, b denotes the false alarm rate, and $0 \le a, b \le 1$. The cost of attacking for malicious node and monitoring for the source, C_a and C_m, are taken into consideration in our model and assumed proportional to the value set of relay R_i, denoted by $C_a(\alpha_I I_i + \alpha_S S_i)$ and $C_m(\alpha_I I_i + \alpha_S S_i)$. $C_f(\alpha_I I_i + \alpha_S S_i)$ denotes the loss of the source caused by false alarm. Table 2 illustrates the utility matrix of attacker and source on relay R_i with probability $1 - \mu_i^{t_k}$ being cooperative at stage t_k.

3.3 Bayesian updating rule on beliefs in the maliciousness of relays

In this section, we define a Bayesian updating rule on beliefs in the maliciousness of relays, which is based on the source's initial beliefs and the source's record of attacker's attacking histories on relays [24,25].

For a given relay R_i, we define a sequence of random variables $T_i^{t_1}, T_i^{t_2}, \ldots$, where $T_i^{t_k}$ characterizes the belief in the cooperativeness of relay R_i at stage t_k. For instance, suppose that at stage t_k, $M_i^{t_k}$ packets have been sent by the source through selected relay R_i to the destination, let $N_i^{t_k}$ be the number of packets successfully forwarded by the selected relay R_i to the destination, out of the $M_i^{t_k}$ packets sent to the selected relay R_i for forwarding at stage t_k. Suppose a prior probability density function for $T_i^{t_{k-1}}$, denoted by $f_i^{t_{k-1}}(m,n,t)$, is known, the posterior probability density function $f_i^{t_k}(m,n,t)$, given the number of received packets $M_i^{t_k}$ and forwarded packets $N_i^{t_k}$, can be obtained as follows:

$$f_i^{t_k}(m,n,t) = \frac{f_i^{t_k}(N_i^{t_k} = n \mid t, M_i^{t_k} = m) f_i^{t_{k-1}}(m,n,t)}{\int_0^1 f_i^{t_k}(N_i^{t_k} = n \mid t, M_i^{t_k} = m) f_i^{t_{k-1}}(m,n,t)dt}, \tag{1}$$

where $f_i^{t_k}(N_i^{t_k} = n \mid t, M_i^{t_k} = m)$ is called the likelihood function and defined as follows:

Table 1 Utility matrix of attacker and source on relay R_i with probability $\mu_i^{t_k}$ malicious at stage t_k

	Attack	Not attack
Select	$-(1-2a-C_a)A_i, (1-2a-C_a)A_i$	$-(bC_f + C_m)A_i, 0$
Not select	$-A_i, (1-C_a)A_i$	$0, 0$

Table 2 Utility matrix of attacker and source on relay R_i with probability $1 - \mu_i^{t_k}$ cooperative at stage t_k

	Not attack
Select	$-(bC_f + C_m)A_i, 0$
Not select	$0, 0$

$$f_i^{t_k}(N_i^{t_k} = n \mid t, M_i^{t_k} = m) = \binom{m}{n} t^n (1-t)^{m-n}. \tag{2}$$

It can be shown that the posterior probability density function $f_i^{t_k}(m,n,t)$ follows a Beta distribution. The Beta distribution with parameters a and b is defined as follows:

$$\text{Beta}(a, b) = \frac{t^{a-1}(1-t)^{b-1}}{B(a, b)} = \frac{t^{a-1}(1-t)^{b-1}}{\int_0^1 t^{a-1}(1-t)dt} \tag{3}$$

for $0 \le t \le 1$. In particular, if

$$f_i^{t_{k-1}}(m,n,t) \sim \text{Beta}(a_i^{t_{k-1}}, b_i^{t_{k-1}}), \tag{4}$$

then given that $M_i^{t_k} = m_i^{t_k}$ and $N_i^{t_k} = n_i^{t_k}$, we have

$$f_i^{t_k}(m,n,t) \sim \text{Beta}(a_i^{t_{k-1}} + n_i^{t_k}, b_i^{t_{k-1}} + m_i^{t_k} - n_i^{t_k}). \tag{5}$$

Therefore, $f_i^{t_k}(m,n,t)$ is characterized by the parameters $a_i^{t_k}$ and $b_i^{t_k}$, which are defined recursively as follows:

$$a_i^{t_k} = a_i^{t_{k-1}} + n_i^{t_k} \tag{6}$$

and

$$b_i^{t_k} = b_i^{t_{k-1}} + m_i^{t_k} - n_i^{t_k}. \tag{7}$$

Therefore, belief in the maliciousness of relay R_i at stage t_k is

$$\mu_i^{t_k} = 1 - f_i^{t_k}(m,n,t), \tag{8}$$

which could be calculated recursively through the record of a_i and b_i [26].

At the system initial stage t_0, there is no information for the cooperative wireless communication networks. Therefore, we assume that $T_i^{t_0}$ has the uniform distribution over the interval [0, 1], i.e.,

$$f_i^{t_0}(m,n,t) \sim U[0, 1] = \text{Beta}(1, 1), \tag{9}$$

which indicates the source's indifference to the selected relay's behavior at stage t_0.

3.4 Finding Nash equilibrium of the proposed game-theoretic approach

In cooperative wireless communication networks, both the attacker and the source have limited system resources, such as limited battery life and limited computational capacity; it is natural for the attacker to focus on attacking some targets that are more beneficial compared by initiating attack on others. We sort the targets according to their combination of information and security assets and divide the whole target set into three subsets: sensible, quasi-sensible, and non-sensible target sets according

to the weight of each relay's asset over the overall assets composed by all relays that belong to $\mathcal{R}$.

The sensible target set $\mathcal{R}_S$, the quasi-sensible target set $\mathcal{R}_Q$, and non-sensible target set $\mathcal{R}_N$ are defined as follows:

$$\begin{cases} \alpha_I I_i + \alpha_S S_i > \frac{|\mathcal{R}_S|(1-C_a)-2a}{(1-C_a)\sum_{j\in\mathcal{R}_S}\frac{1}{\alpha_I I_j+\alpha_S S_j}}, & \forall i \in \mathcal{R}_S \\ \alpha_I I_i + \alpha_S S_i = \frac{|\mathcal{R}_S|(1-C_a)-2a}{(1-C_a)\sum_{j\in\mathcal{R}_S}\frac{1}{\alpha_I I_j+\alpha_S S_j}}, & \forall i \in \mathcal{R}_Q \\ \alpha_I I_i + \alpha_S S_i < \frac{|\mathcal{R}_S|(1-C_a)-2a}{(1-C_a)\sum_{j\in\mathcal{R}_S}\frac{1}{\alpha_I I_j+\alpha_S S_j}}, & \forall i \in \mathcal{R}_N \end{cases} \quad (10)$$

where $|\mathcal{R}_S|$ is the cardinality of $\mathcal{R}_S$.

The cardinality of $\mathcal{R}_S$ could be calculated as follows:

1. If $\alpha_I I_K + \alpha_S S_K > \frac{K(1-C_a)-2a}{(1-C_a)\sum_{j=1}^{|\mathcal{R}|}\frac{1}{\alpha_I I_j+\alpha_S S_j}}$, then $|\mathcal{R}_S| = K$ and $|\mathcal{R}_Q| = 0$.
2. If $\alpha_I I_K + \alpha_S S_K \le \frac{K(1-C_a)-2a}{(1-C_a)\sum_{j=1}^{|\mathcal{R}|}\frac{1}{\alpha_I I_j+\alpha_S S_j}}$, $|\mathcal{R}_S|$ is determined by the following formulas:

$$\begin{cases} \alpha_I I_{|\mathcal{R}_S|} + \alpha_S S_{|\mathcal{R}_S|} > \frac{|\mathcal{R}_S|(1-C_a)-2a}{(1-C_a)\sum_{j=1}^{|\mathcal{R}_S|}\frac{1}{\alpha_I I_j+\alpha_S S_j}} \\ \alpha_I I_{|\mathcal{R}_S|+1} + \alpha_S S_{|\mathcal{R}_S|+1} \le \frac{|\mathcal{R}_S|(1-C_a)-2a}{(1-C_a)\sum_{j=1}^{|\mathcal{R}_S|}\frac{1}{\alpha_I I_j+\alpha_S S_j}} \end{cases} \quad (11)$$

Quasi-sensible target set $\mathcal{R}_Q$ consists of relay nodes whose assets are equal to

$$\frac{|\mathcal{R}_S|(1-C_a)-2a}{(1-C_a)\sum_{j=1}^{|\mathcal{R}_S|}\frac{1}{\alpha_I I_j+\alpha_S S_j}}. \quad (12)$$

The first step in finding the Nash equilibrium of the proposed dynamic Bayesian game-theoretic approach used for modeling the interactions between the source and the attacker is to apply *Harsanyi* transformation that converts the incomplete information game into a normal form game. Given that the Harsanyi transformation is a standard concept in the game theory, we introduce it literally without introducing a mathematical formula concerning Harsanyi transformation [27]. For each relay, there are two possible types, malicious with probability $\mu_i^{t_k}$ and cooperative with probability $1-\mu_i^{t_k}$. We combine the utility matrix of Table 1 and the utility matrix of Table 2 to obtain Table 3 whose components are expected utilities of malicious type relay and cooperative type relay. There are two combined attacking strategies for the attacker: Attack and Not attack*, and Not attack and Not attack*, in which Not attack* is the pure strategy of the attacker on cooperative relay.

Table 3 Utility matrix of attacker and source on relay R_i at stage t_k after Harsanyi transformation

	Attack, Not attack*	Not attack, Not attack*
Select	$-\mu_i^{t_k}(1-2a+C_m)A_i-(1-\mu_i^{t_k})\times(bC_f+C_m)A_i, \mu_i^{t_k}(1-2a-C_a)A_i$	$-(bC_f+C_m)A_i, 0$
Not select	$-\mu_i^{t_k}A_i, \mu_i^{t_k}(1-C_a)A_i$	$0, 0$

Denote the total utility for the attacker and the source by $U_A^{t_k}(P,Q)$ and $U_S^{t_k}(P,Q)$ at stage t_k as:

$$\begin{aligned} U_A^{t_k}(P,Q) &= \sum_{i\in\mathcal{R}} p_i q_i \mu_i^{t_k}[(1-2a)A_i - C_a A_i] \\ &\quad + p_i(1-q_i)\mu_i^{t_k}(1-C_a)A_i \\ &= \sum_{i\in\mathcal{R}} p_i A_i \mu_i^{t_k}(1-2aq_i-C_a), \end{aligned} \quad (13)$$

$$\begin{aligned} U_S^{t_k}(P,Q) &= \sum_{i\in\mathcal{R}} p_i q_i[-\mu_i^{t_k}(1-2a+C_m)A_i \\ &\quad -(1-\mu_i^{t_k})(bC_f+C_m)A_i] - p_i(1-q_i)\mu_i^{t_k}A_i \\ &\quad -(1-p_i)q_i(bC_f+C_m)A_i \\ &= \sum_{i\in\mathcal{R}} q_i A_i[p_i\mu_i^{t_k}(2a+bC_f)-(bC_f+C_m)] \\ &\quad - p_i\mu_i^{t_k}A_i. \end{aligned} \quad (14)$$

The attacker and the source select their strategies P^* and Q^* to maximize $U_A^{t_k}(P,Q)$ and $U_S^{t_k}(P,Q)$.

Similar to the Nash equilibrium obtained from the proposed static game-theoretic approach, it holds that

$$\begin{aligned} 0 &\le (1-2aq_i^*-C_a)A_i\mu_i^{t_k} = (1-2aq_j^*-C_a)A_j\mu_j^{t_k} \\ &\ge (1-2aq_k^*-C_a)A_k\mu_k^{t_k} \forall i,j,k \in \mathcal{R}, p_i^*, p_j^* > 0, p_k^* = 0, \end{aligned} \quad (15)$$

which can be shown by noticing the attacker's total utility function $U_A^{t_k}(P,Q)$: if $(1-2aq_i^*-C_a)A_i\mu_i^{t_k} < 0$, then the attacker has the incentive to change p_i^* to 0; if $(1-2aq_i^*-C_a)A_i\mu_i^{t_k} < (1-2aq_j^*-C_a)A_j\mu_j^{t_k}$, then the attacker is inclined to decrease p_i^* and increase p_j^*; and if $(1-2aq_j^*-C_a)A_j\mu_j^{t_k} < (1-2aq_k^*-C_a)A_k\mu_k^{t_k}$, then the attacker obtains more utility by adding p_i^* to p_k^* and setting p_i^* equal to 0. Similarly, noticing the source's total utility function $U_S^{t_k}(P,Q)$, it holds that

$$\begin{aligned} 0 &\le A_i\mu_i^{t_k}[p_i^*(2a+bC_f)-(bC_f+C_m)] \\ &= A_j\mu_j^{t_k}[p_j^*(2a+bC_f)-(bC_f+C_m)] \\ &\ge A_k\mu_k^{t_k}[p_k^*(2a+bC_f)-(bC_f+C_m)] \\ &\quad \forall i,j,k \in \mathcal{R}, q_i^*, q_j^* > 0, q_k^* = 0. \end{aligned} \quad (16)$$

To find the Nash equilibrium (P^*, Q^*) of the proposed dynamic Bayesian game-theoretic approach, we need to reclaim that $A_i > A_j$ if $i > j$ and $\sum_i^{|\mathcal{R}|} p_i^* = \sum_i^{|\mathcal{R}|} q_i^* = 1$.

From

$$(1 - 2aq_i^* - C_a)A_i\mu_i^{t_k} = (1 - 2aq_j^* - C_a)A_j\mu_j^{t_k}, \quad (17)$$

$$\begin{aligned} &A_i\mu_i^{t_k}[p_i^*(2a + bC_f) - (bC_f + C_m)] \\ &= A_j\mu_j^{t_k}[p_j^*(2a + bC_f) - (bC_f + C_m)], \end{aligned} \quad (18)$$

we have

$$p_i^* = \frac{bC_f + C_m}{\mu_i^{t_k}(2a + bC_f)} + \frac{A_j[p_j\mu_j^{t_k}(2a + bC_f) - (bC_f + C_m)]}{A_i\mu_i^{t_k}(2a + bC_f}), \quad (19)$$

$$q_i^* = \frac{1}{2a}[\,1 + C_a - \frac{A_j\mu_j^{t_k}(1 - 2aq_j + C_a)}{A_i\mu_i^{t_k}}]. \quad (20)$$

For the proposed dynamic Bayesian game-theoretic approach, Nash equilibrium (P^*, Q^*) at stage t_k is given as follows:

$$p_i^* \begin{cases} = \frac{1}{A_i\mu_i^{t_k}\sum_1^{|\mathcal{R}_S|}\frac{1}{A_i\mu_i^{t_k}}} - (\frac{\sum_1^{|\mathcal{R}_S|}\frac{1}{\mu_i^{t_k}}}{A_i\mu_i^{t_k}\sum_1^{|\mathcal{R}_S|}\frac{1}{A_i\mu_i^{t_k}Y}} - \frac{1}{\mu_i^{t_k}})\frac{bC_f + C_m}{2a + bC_f} & i \in \mathcal{R}_S \\ \in [0, \frac{1}{A_i\mu_i^{t_k}\sum_1^{|\mathcal{R}_S|}\frac{1}{A_i\mu_i^{t_k}}}(\frac{\sum_1^{|\mathcal{R}_S|}\frac{1}{\mu_i^{t_k}}}{A_i\mu_i^{t_k}\sum_1^{|\mathcal{R}_S|}\frac{1}{A_i\mu_i^{t_k}}} - \frac{1}{\mu_i^{t_k}})\frac{bC_f + C_m}{2a + bC_f}] & i \in \mathcal{R}_Q \\ = 0 & i \in \mathcal{R}_N \end{cases} \quad (21)$$

$$q_i^* = \begin{cases} \frac{1}{2a}(1 - C_a - \frac{|\mathcal{R}_S|(1 - C_a) - 2a}{A_i\mu_i^{t_k}\sum_1^{|\mathcal{R}_S|}\frac{1}{A_i\mu_i^{t_k}}}) & i \in \mathcal{R}_S \\ 0 & \text{otherwise} \end{cases} \quad (22)$$

where

$$\sum_{i \in \mathcal{R}} p_i^* = \sum_{i \in \mathcal{R}} q_i^* = 1. \quad (23)$$

Nash equilibrium (P^*, Q^*) of the proposed static game-theoretic approach is the special case of the Nash equilibrium of the proposed dynamic Bayesian game-theoretic approach by setting μ_i equal to 1, which assumes that all candidate relay nodes are completely malicious.

3.5 System performance analysis

In our model, the system security requirement is defined as the maximum percentage of packets forwarded to the destination through the selected relay that are compromised by the attacker if the attacker's attacking target selection coincides with the source's relay selection. Denote the utility brought by a successful attack on targeted relay R_i as $u_A(p_i, q_i)$. We assume that the attacker prefers selecting relay R_i with the attacking probability p_i^* that maximizes $u_A(p_i, q_i)$ as its attacking target; the attacker's attacking target selection may coincide with the source's relay selection. If the attacker's selection coincides with the relay selection of the source, then both identity-authentication and packet-integration checking processes are needed to guarantee a secured communication. However, when a decision on relay selection is made, the source could not make sure which relay is the target of the attacker except for a probability of being attacked, but the source could detect the attack initiated by the attacker on relays. Therefore, with the satisfaction of the system security requirement, the source would not necessarily authenticate all packets, according to the possibility that packets forwarded by the selected relay are not compromised by the attacker because the source's relay selection is different from the attacker's attacking target selection. Since not all the packets sent by the source are needed to be authenticated, compared with the stringent authentication relay selection method [28], which authenticates all transmitted packets, the proposed game-theoretic approach provides a quantitative approach to calculate the authentication probability based on the attacker's attacking probabilities on relays and system security requirement and to avoid the unnecessary consumption of system resources.

Denote the probability of message authentication as p_a. To satisfy system security requirement p_s, we have $0 \leq (1 - p_a) \cdot p_i^* \leq p_s$ by selecting relay R_i as relay with probability p_i^* being attacked by the attacker.

3.5.1 Outage probability and capacity

In the proposed game-theoretic approach, denote I_i as the maximum value between the mutual information of direct communication I_{DC} and the minimal value between I_{SR_i}, the mutual information between the source and the selected relay R_i, and I_{MRC}, the mutual information sum of source destination and relay R_i destination [29]. We define SNR as the average signal-to-noise ratio from the source node to the destination node [16]. I_{DC} is given by:

$$I_{\mathrm{DC}} = \log_2(1 + |h_{\mathrm{SD}}|^2\mathrm{SNR}) \quad (24)$$

and I_{SR_i} is given by:

$$I_{SR_i} = \frac{1}{2}\log_2(1 + |h_{SR_i}|^2 \mathrm{SNR}), \tag{25}$$

where $|h_{SR_i}|$ is the channel between the source and relay R_i. Given the half-duplex constraint in cooperative wireless communication networks which means a relay could not transmit and receive signal simultaneously, the factor $\frac{1}{2}$ mirrors the two time slots for relaying. I_{MRC} is given by:

$$I_{\mathrm{MRC}} = \frac{1}{2}\log_2(1 + (|h_{\mathrm{SD}}|^2 + |h_{R_iD}|^2)\mathrm{SNR}), \tag{26}$$

where $|h_{\mathrm{SD}}|$ is the channel between the source and the destination and $|h_{R_iD}|$ is the channel between the selected relay R_i and the destination.

Suppose the data transmission rate between the source and the destination is r, the outage probability $P_{\mathrm{out}}^{I_i}$ is defined as the probability that the mutual information I_i between the source and the destination through relay R_i is lower than the transmission data rate r, i.e., $P_{\mathrm{out}}^{I_i} = P\{I_i < r\}$, which characterizes the probability of transmission data loss.

In the case of the proposed game-theoretic approach, the outage probability is defined as follows:

$$P_{\mathrm{out}}^{I_i} = P\{\max\{I_{\mathrm{DC}}, \min\{I_{SR_i}, I_{\mathrm{MRC}}\}\} < r\}, \tag{27}$$

from which we can obtain,

$$P_{\mathrm{out}}^{I_i} = 1 - \nu + \frac{\omega^{(d_{SR_i}^{\alpha} + d_{R_iD}^{\alpha})}(\nu^{(1-d_{R_iD})} - 1)}{1 - d_{R_iD}^{\alpha}}, \tag{28}$$

where ω equals to $\exp(2\ln\nu - (\ln\nu)^2\gamma)$ and ν equals to $\exp(-\frac{2^r-1}{\gamma})$. d_{SR_i} denotes the distance between the source and selected relay R_i, d_{R_iD} denotes the distance between selected relay R_i and the destination, and γ denotes the average transmitted SNR between any nodes.

The outage capacity C_{ϵ}^{I} is defined as the largest data transmission rate r that can be supported if the outages are allowed to occur with a certain probability ϵ, which is the probability that the transmission cannot be decoded with negligible error probability. Solving $P_{\mathrm{out}}^{I_i} = \epsilon$, we have ν_{ϵ}. Thus, we have

$$C_{\epsilon}^{I} = \log_2(1 + \gamma\ln(\frac{1}{\nu_{\epsilon}, \gamma})). \tag{29}$$

Outage capacity is used instead of Shannon capacity in slow-fading channel since the slow-fading channel is different from the additive white Gaussian noise channel as delay constraints on the order of channel coherence time.

3.5.2 Bit error rate

Bit error rate (BER) is the percentage of bits that has errors relative to the total number of bits sent in a transmission. The end-to-end BER, is given by:

$$P_e^{I_i} = P_{\mathrm{out}}^{SR_i} \cdot P_e^{\mathrm{DC}} + (1 - P_{\mathrm{out}}^{SR_i}) \cdot P_e^{\mathrm{div},i}, \tag{30}$$

where $P_{\mathrm{out}}^{SR_i}$ is the outage probability of the link from the source to the selected relay R_i [30], P_e^{DC} is the probability of error in direct communication form source to destination over Rayleigh channel, and $P_e^{\mathrm{div},i}$ is the probability that an error occurs in combined transmission from the source to the destination through the selected relay R_i. $P_{\mathrm{out}}^{SR_i}$ is given as follows:

$$P_{\mathrm{out}}^{SR_i} = 1 - \exp(-(\frac{2^{2r}-1}{\overline{\gamma_{SR_i}}})). \tag{31}$$

P_e^{DC} is given by:

$$P_e^{\mathrm{DC}} = \frac{1}{2}(1 - \sqrt{\frac{\overline{\gamma_{\mathrm{SD}}}}{1 + \overline{\gamma_{\mathrm{SD}}}}}). \tag{32}$$

$P_e^{\mathrm{div},i}$ is given as follows:

$$P_e^{\mathrm{div},i} = \frac{1}{2}[1 + \frac{1}{\overline{\gamma_{R_iD}} - \overline{\gamma_{\mathrm{DC}}}}(\frac{\overline{\gamma_{\mathrm{DC}}}}{\sqrt{1 + \frac{1}{\overline{\gamma_{\mathrm{DC}}}}}} - \frac{\overline{\gamma_{R_iD}}}{\sqrt{1 + \frac{1}{\overline{\gamma_{R_iD}}}}})], \tag{33}$$

where $\overline{\gamma_{\mathrm{DC}}}$ denotes the SNR between the source and the destination and $\overline{\gamma_{R_iD}}$ denotes the SNR between the selected relay R_i and the destination.

3.5.3 System throughput

We derive the throughput for partial authentication process with ALPHA-M protocol [10] and modify it to cover both direct communication and source-relay-destination communication. Furthermore, we formulate the throughput equations for both selective repeat [31] and Go-Back-N [32] automatic repeat request retransmission schemes by taking the error rate into consideration.

The payload for packets with authentication is given as follow:

$$S_{\mathrm{payload}} = n \cdot p_a \cdot (S_{\mathrm{packet}} - S_h(\lceil\log_2(n)\rceil + 1)), \tag{34}$$

where S_{payload} is the amount of payload that can be transmitted with a single pre-signature, n is the number of data blocks at the bottom of the Merkle tree, S_{packet} is the size of packet, and S_h is the hash output [10].

The payload for packets without authentication is

$$S'_{\mathrm{payload}} = n \cdot (1 - p_a) \cdot (S_{\mathrm{packet}} - S_h). \tag{35}$$

Generally, throughput is defined as the payload divided by the total time used for processing and transmitting the payload. In our case, the total time spent on payload processing and transmitting consists of two parts: T_1, the time for the initial pre-signature process between the source

Table 4 Time parameters in T_1

	t_{prop1}	t_{f1}	t_{proc1}	t_{ack1}
T_1^{DC}	$2(\frac{d_{SD}}{c})$	1	3	1
T_1^{SRD}	$2(\frac{d_{SR_i}}{c}) + 2(\frac{d_{R_iD}}{c})$	2	5	2

and the destination, and T_2, the time for the actual authenticated and non-authenticated message transmission and delivery. The general throughput T could then be defined as:

$$\mathrm{T} = \frac{S_{\text{payload}} + S'_{\text{payload}}}{T_1 + T_2}. \tag{36}$$

The values for the time parameters in T_1 and T_2 vary according to two communication paths, direct communication and source-relay-destination, which are presented in Tables 4 and 5.

The message sequence charts that show the transmission of message from the source to the destination and acknowledgment between the destination and the source with and without the use of relay are shown in Figure 3.

The parameters presented in Tables 4 and 5 are explained as follows:

- t_{prop1} is the propagation time for the S_1 packet from the source to the destination or the propagation time for the A_1 packet sent from the destination to the source. In the case of direct communication, t_{prop1} is given by $\frac{d_{\text{SD}}}{c}$, where d_{SD} is the distance between the source and the destination and c is the speed of light. In the case of source-relay-destination, this consists of the time for the S_1 packet sent from the source to the selected relay R_i and from the selected relay R_i to the destination or for the A_1 packet sent from the destination to the selected relay R_i and from the selected relay R_i to the source, which is given by the sum of $\frac{d_{SR_i}}{c}$ and $\frac{d_{R_iD}}{c}$.
- t_{prop2} is the propagation time for the S_2 packet from the source to the destination or for the A_2 packet from the destination to the source. In the case of direct communication, this is given by $\frac{d_{\text{SD}}}{c}$. In case of source-relay-destination, this consists of the propagation time for the S_2 packet from the source to the selected relay R_i and from the selected relay R_i to the destination or for the A_2 packet from the destination to the selected relay R_i and from the selected relay R_i to the source, which is given by the sum of $\frac{d_{SR_i}}{c}$ and $\frac{d_{R_iD}}{c}$.
- t_{f1} is the packet transmission time for the S_1 packet, which is given by $\frac{u_{\text{f1}}}{r}$. u_{f1} is the number of bits in the S_1 packet, and r is the data transmission rate.
- t_{f2} is the packet transmission time for the S_2 packet, which is given by $\frac{u_{\text{f2}}}{r}$. u_{f2} is the number of bits in the S_2 packet, and r is the data transmission rate.
- t_{ack1} is the packet transmission time for the A_1 packet, which is given by $\frac{u_{\text{ack1}}}{r}$. u_{ack1} is the number of bits in the A_1 packet, and r is the data transmission rate.
- t_{ack2} is the packet transmission time for the A_2 packet, which is given by $\frac{u_{\text{ack2}}}{r}$. u_{ack2} is the number of bits in the A_2 packet, and r is the data transmission rate.
- t_{proc1} is the processing time at the source and the destination for S_1 and A_1 packets in direct communication, which includes the Merkle tree generating time for S_1 packet at the source and the acknowledgment Merkle tree for A_1 packet at the destination along with processing at the selected relay R_i in source-relay-destination.
- t_{proc2} is the processing time at the source and the destination for S_2 and A_2 packets in direct communication, along with processing time at the selected relay R_i in source-relay-destination.

Table 5 Time parameters in T_2

	t_{prop2}	t_{f2}	t_{proc2}	t_{ack2}
T_2^{DC}	$2(\frac{d_{SD}}{c})$	n	1	1
T_2^{SRD}	$2(\frac{d_{SR_i}}{c}) + 2(\frac{d_{R_iD}}{c})$	$n+1$	3	2

Wireless channels have high error rates due to multipath fading which characterizes mobile radio channels. However, many networks require that the error rates should be significantly small. In addition to the poor channel quality, the design of wireless communication systems is complicated by the rapidly changing quality of the radio channel [33]. To increase the apparent quality of a communication channel, two distinct approaches are used:

- Forward error correction which employs error-correcting codes to combat bit errors which are due to channel imperfections by adding redundancy, such as henceforth parity bits, to information packets before they are transmitted. This redundancy is used by the receiver to detect and correct errors that are introduced in the transmission process.
- Automatic repeat request (ARQ) wherein only error detection capability is provided and no attempt to correct any packets received in error is made. Packets received in error are retransmitted by the sender.

In the throughput analysis, ARQ retransmission is incorporated, and the following is a brief review of three typical ARQ retransmission schemes [34].

- *Stop and wait (SW) ARQ*. When using the SW ARQ scheme, the sender transmits a packet only when all

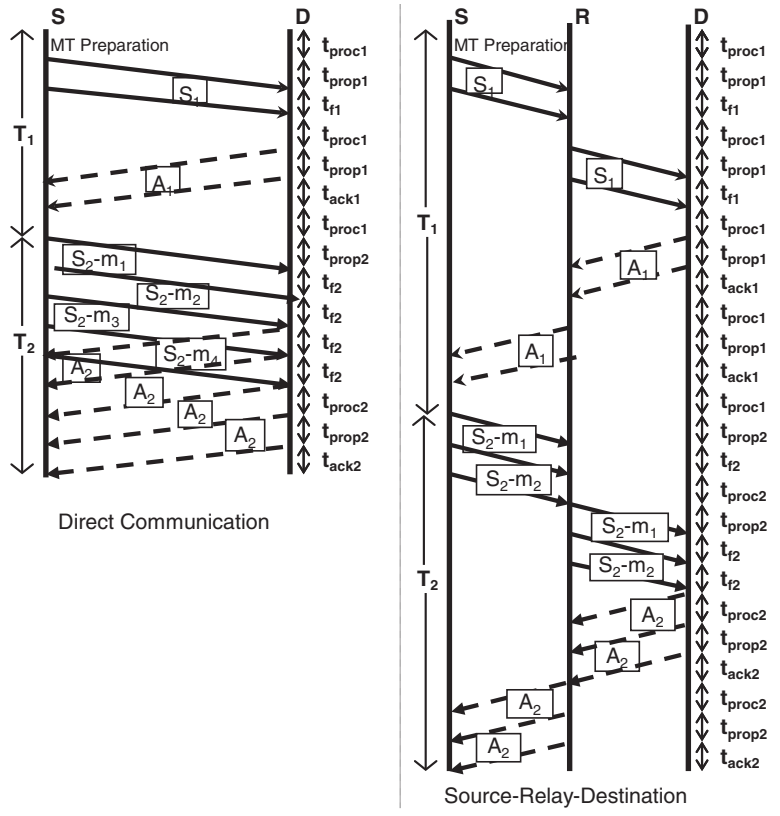

Figure 3 Message sequence charts in direct communication and source-relay-destination communication.

previously transmitted packets have been successfully acknowledged by the receiver. Hence, when using SW ARQ scheme, the sender, after transmitting a packet, waits for its acknowledgment. Once its acknowledgment has been received, the next packet is transmitted. However, if an acknowledgment does not arrive until a timeout timer expires, the packet is retransmitted by the sender. Therefore, in SW ARQ, there is never more than a single packet that is unacknowledged at any given instant of time. Since the sender does not use the available channel during time intervals, it waits for an acknowledgment and the maximum data transfer rate that can be supported is limited. This limits cases where the SW ARQ protocol can be employed. Huge buffer is needed to buffer unacknowledged packets.

- *Selective repeat (SR) ARQ.* Unlike SW ARQ, when using SR ARQ, packets are transmitted continuously by the sender. As before, the receiver acknowledges each successfully received packet by transmitting an ACK bearing the sequence number of the packet being acknowledged. If an acknowledgment is not received for a packet before the expiration of the timeout, the packet is retransmitted. Once a packet has been retransmitted, the sender resumes transmission of packets from where it is left off, i.e., if a is the packet with the largest sequence number that has been transmitted, packet with sequence number $a + 1$ is transmitted next. Here, we assume that no other timers have expired in the meantime. Since the SR ARQ protocol is employed, packets are continuously being transmitted and the inefficiency associated with SW ARQ is eliminated. Observe that when SR ARQ is employed, packets can be accepted out of sequence. Hence, packets received out of sequence have to be buffered and sequenced before they can be delivered.
- *Go-Back-N (GBN) ARQ.* When GBN ARQ is employed, packets are transmitted continuously as in SR ARQ. However, the receiver accepts packets only in the order in which they were transmitted. Packets received out of sequence are discarded and not acknowledged. Since the receiver accepts packets only in sequence, after a timeout, the sender retransmits the packet that timed out and all packets with sequence numbers that follow the one that was retransmitted. Hence, each time a timeout occurs, all packets that are yet to be acknowledged are retransmitted. It is important to observe that GBN ARQ attempts to combine the desirable features of

SR and SW ARQs, i.e., packets are transmitted continuously, as in SR ARQ, without the need to buffer out-of-sequence packets and there is no re-sequencing overhead.

To incorporate the error control schemes into our throughput equation, we expand the general throughput equation by including the error rate. Define the packet error rate P_c as the probability that the received packet with the length of S_{packet} bits contains no error as $P_c = (1 - P_e^{I_i})^{S_{\text{packet}}}$. Let T_{SR} denote the modified throughput with SR ARQ, which is given as follows:

$$\text{T}_{\text{SR}} = \frac{(S_{\text{payload}} + S'_{\text{payload}}) \cdot P_c}{T_1 + T_2}. \tag{37}$$

Concerning the GBN ARQ, the throughput equation is further modified to allow the retransmission of an error frame along with all frames that have been transmitted until the time a negative acknowledgment is received from the destination. Thus, the modified throughput with GBN ARQ, denoted by T_{GBN}, is given as:

$$\text{T}_{\text{GBN}} = \frac{(S_{\text{payload}} + S'_{\text{payload}}) \cdot P_c}{T_1 + T_2[P_c + (1 - P_c)W_s]}, \tag{38}$$

where W_s is the window size which is calculated by dividing the product of the data rate of the transmission channel and the reaction time by the packet size.

3.5.4 Optimizing the number of messages

Besides strategically selecting relay, the source also needs to determine the optimal number of messages once its relay is selected. For various packet sizes S_{packet} and authentication probability p_a, the optimal value of the number of messages n that results in the highest throughput is denoted as n^*. The optimal number of messages for selected relay R_i is driven from:

$$n^* = \arg\max_n \text{T}(R_i, S_{\text{packet}}, n, p_a), \tag{39}$$

where $n \in \{1, 2, \ldots\}$ for the selected relay R_i.

4 Simulation results and discussions

In this section, we evaluate the performance of the proposed game-theoretic approach for security and QoS co-design in cooperative wireless communication networks through extensive simulations using matrix laboratory (MATLAB, Mathworks, Natick, MA, USA). All simulations are executed on a laptop featured with Windows 7 (Microsoft, Redmond, WA, USA), Intel Core Duo 2.1 GHz CPU (Santa Clara, CA, USA), 2-GB memory, and MATLAB R2010b. As illustrated in Figure 4, we set up a network topology with the source and the destination located 1,000 m apart in two separate corners and four relays randomly located between the source and the destination in an area of $1,000 \times 300$ m^2. We set the transmission data rate equal to 1 Mbps, path loss exponent equal to 3.5, and fixed outage probability equal to 0.01.

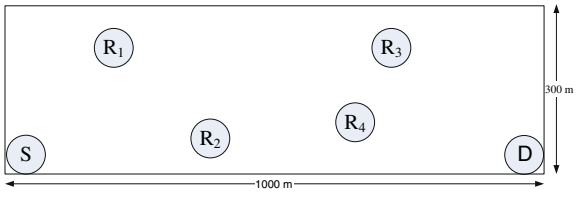

Figure 4 Simulation topology.

Table 6 Nash equilibrium and players' utility in the military network

Nash equilibrium	Players' utility
$p_1^* = 0.23256, q_1^* = 0.4$	$u_A(p_1^*, q_1^*) = 0.062792, u_D(p_1^*, q_1^*) = -0.069271$
$p_2^* = 0.30814, q_2^* = 0.35$	$u_A(p_2^*, q_2^*) = 0.083198, u_D(p_2^*, q_2^*) = -0.088225$
$p_3^* = 0.4593, q_3^* = 0.25$	$u_A(p_3^*, q_1^*) = 0.12401, u_D(p_1^*, q_1^*) = -0.12759$
$p_4^* = 0, q_4^* = 0$	$u_A(p_4^*, q_4^*) = 0, u_D(p_4^*, q_4^*) = 0$

Similar to [35], firstly, we consider a network with emphasis on system security, e.g., military network, where there are tight confidential requirements. In this network, the security asset weights heavier than the information asset and the combined asset is much higher than the attack monitoring cost, e.g., $\alpha_I < \alpha_S$ and $C_a, C_m, C_f \ll 1$. We set $C_a = C_m = 0.01$ and $C_f = 0.01$. Terminals in military network usually own high-performance attack monitoring equipments and powerful processing capability; thus, we set $a = 0.9$ and $b = 0.05$.

Secondly, a network with loose emphasis on system security is considered, e.g., commercial WLAN. In this network, the information asset weights heavier than the security asset and the related attacking and attack monitoring cost is relatively high, i.e., $\alpha_I > \alpha_S$, and we set $C_a = C_m = 0.1$ and $C_f = 0.3$. The terminals in the commercial network are not as efficient as those in the military network; thus, we set $a = 0.6$ and $b = 0.2$.

In both networks, there are four relays with normalized information and security assets: $A_i = (5 - i) \cdot 0.25$, $i = \{1, 2, 3, 4\}$. Tables 6 and 7 show the $\mathbf{NE}(P^*, Q^*)$ of the

Table 7 Nash equilibrium and players' utility in the commercial network

Nash equilibrium	Players' utility
$p_1^* = 0.26984, q_1^* = 0.46154$	$u_A(p_1^*, q_1^*) = 0.093407, u_D(p_1^*, q_1^*) = -0.18676$
$p_2^* = 0.31746, q_2^* = 0.36583$	$u_A(p_2^*, q_2^*) = 0.10989, u_D(p_2^*, q_2^*) = -0.17233$
$p_3^* = 0.4127, q_3^* = 0.17308$	$u_A(p_3^*, q_3^*) = 0.14286, u_D(p_3^*, q_3^*) = -0.1752$
$p_4^* = 0, q_4^* = 0$	$u_A(p_4^*, q_4^*) = 0, u_D(p_4^*, q_4^*) = 0$

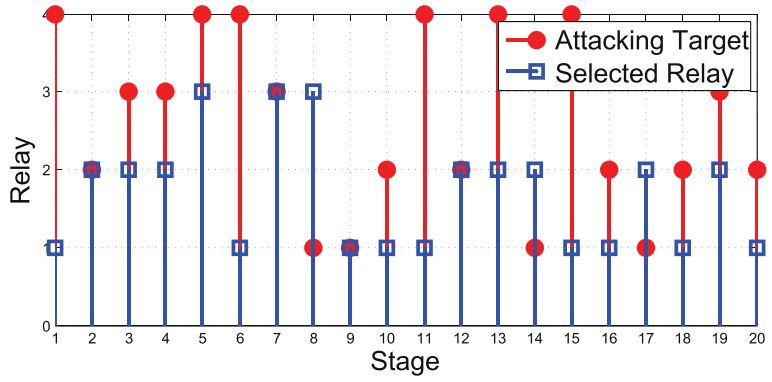

Figure 5 Dynamic attacking target and selected relay.

proposed static game-theoretic approach obtained using analytical results. As shown in Tables 6 and 7, both the attacker and the source focus only on the relays in the sensible target set, which bring them more utility.

The setup of the parameters is a non-trivial task for the proposed scheme. In constructing these parameters, we assume that most network properties can be made known, which should be realistic in practical networks, where initial planning and network management is an *a priori* requirement.

The attacker would choose the relay that brings maximum attacking utility as its attacking target. According to the obtained Nash equilibrium, the attacker in the military network is prone to select relay 3 as its attacking target. However, in the real network, the attacking target is selected randomly by the attacker. To simulate the randomness of attacker's selection on attacking target, we generate random numbers r' that satisfy 0-1 uniform distribution and set following attacking target selection standard, e.g., if $(i-1)*0.25 \leq r' < i*0.25, i = \{1,2,3,4\}$, relay i is selected as attacking target.

In this section, we discuss dynamic beliefs in the maliciousness of relays according to the attacker's attacking histories on relays and dynamic total utility of the source brought by its dynamic beliefs in the maliciousness of relays. At each stage, the source updates its belief in maliciousness of the selected relay according to its record of attacker's attack on the selected relay. At each stage, if the selected relay by the source is also selected by the attacker as attacking target, packets sent to the destination through the selected relay are considered compromised and could not be used by the destination to recover the original information sent by the source; otherwise, packets sent through the selected relay arrive at the destination without being compromised and could be used by the destination to recover the original information.

Figure 5 shows the simulation results of dynamic change of attacking target of the attacker and the dynamic change of the selected relay of the source for the first 20 consecutive stages of the proposed dynamic game-theoretic approach.

Figures 6 and 7 show the dynamic belief change of the source in the maliciousness of relays 1 and 4, respectively. The source updates its beliefs in the maliciousness of relays according to its record of attacker's attack on relays. At the commence of simulations, the source's beliefs in the maliciousness of all relays are unbiased; in another word, belief in the maliciousness and cooperativeness is 50:50. Between every two consecutive stages, the source monitors the attacking target selection of the attacker. If the selected relay by the source is not the attacking target,

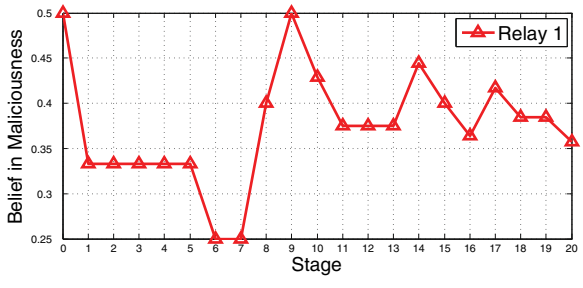

Figure 6 Dynamic belief in the maliciousness of relay 1.

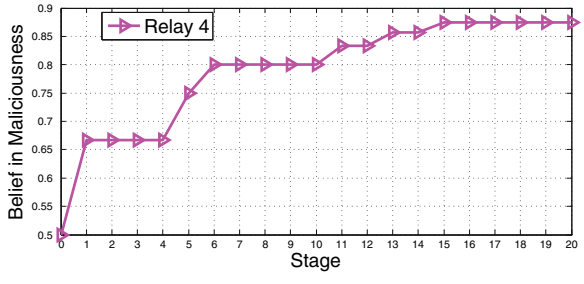

Figure 7 Dynamic belief in the maliciousness of relay 4.

then the source increases its belief in the cooperativeness of the selected relay; if the selected relay is selected as attacking target, then the source increases its belief in the maliciousness of the selected relay; otherwise, other relays are neither selected as relay by the source nor are selected as attacking target by the attacker, and the source's beliefs in the maliciousness or cooperativeness of other relays stay unchanged.

As shown in Figure 5, at stage 1, the observed attacking target is relay 4, and the relay selected by the source is relay 1. At this stage, the attacking target does not coincide with the selected relay. Therefore, the source's belief in the maliciousness of relay 1 decreases, the source's belief in the maliciousness of relay 4 increases, and the source's beliefs in the maliciousness of relays 2 and 3 stay unchanged. Simulation results in Figures 6 and 7 keep consensus with the above analysis. Figure 8 shows the comparison of the total utility of the source in the military and commercial networks in the first 20 stages. The source in the military network has lower monitoring cost C_m and false alarming cost C_f; thus, when each relay is assigned the same amount of combined information and security assets, the total utility obtained by the source in the military network is higher than the total utility obtained by the source in the commercial network.

In this section, we discuss the impact of dynamic belief update in the maliciousness of relays on system throughput and compromising probability of the proposed dynamic game-theoretic approach, which enables the source update its beliefs in the maliciousness of relays based on the attacker's attacking histories on selected relays. Numerous simulations are executed to draw reliable results concerning the impact of dynamic beliefs in the maliciousness of relays on throughput and compromising probability.

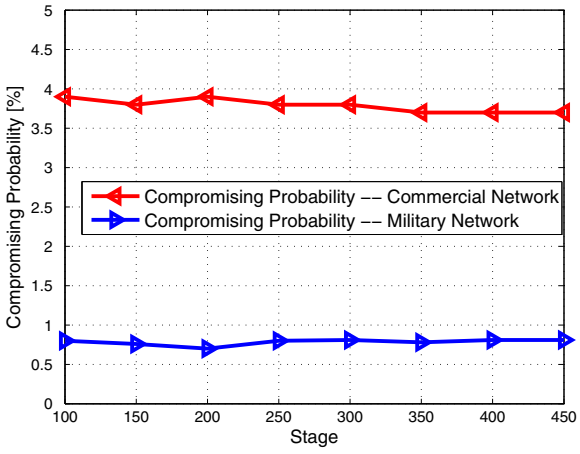

Figure 9 Dynamic compromising probability comparison between the military and commercial networks.

Compromising probability comparison between the military and commercial networks is shown in Figure 9. From Figure 9, we can see that the compromising probability of the military network is smaller than that of the commercial network. Since the security requirement of the military network is more stringent than the security requirement of the commercial network, the authentication probability of the military network is higher than the authentication probability of the commercial network. Figure 10 shows the throughput comparison between the military and commercial networks. From Figure 10, we can see that the system throughput of the commercial network is higher than that of the military network due to the higher authentication probability of the military network.

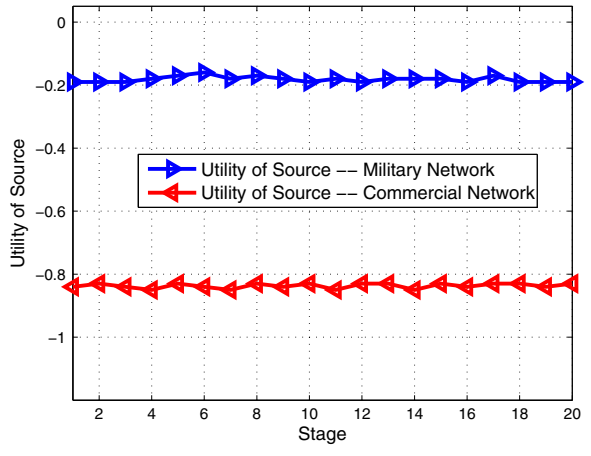

Figure 8 Comparison of dynamic total utility of the source in the military and commercial networks.

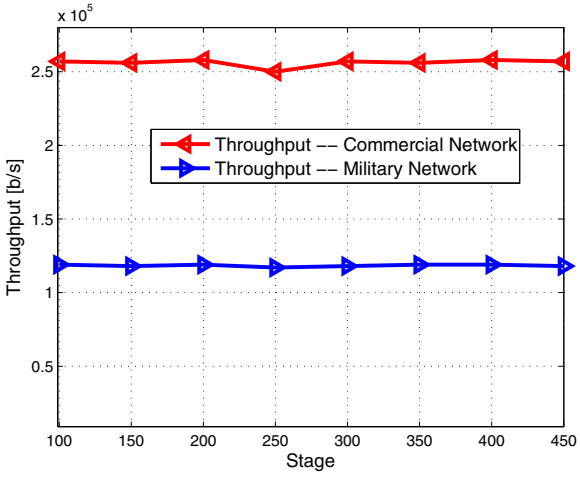

Figure 10 Dynamic throughput comparison between the military and commercial networks (SNR = 30 dB).

5 Conclusions

In this paper, we have proposed a game theoretical approach for security and QoS co-design in MANETs with cooperative communications. With the consideration of system throughput and system security requirement, the proposed game theoretical approach enables the system to strategically select its relay by dynamically updating its belief in the maliciousness of relays according to its record of attacks. Simulation results have been presented to show the effectiveness of the proposed dynamic game-theoretic approach. Future work is in progress to consider multi-hop/multirelay cooperative communications in MANETs.

Competing interests
The authors declare that they have no competing interests.

Author details
[1]Department of Systems and Computer Engineering, Carleton University, Ottawa, ON K1S 5B6, Canada. [2]Defence Research and Development Canada-Ottawa, Ottawa, ON K1A 0Z4, Canada.

Received: 16 January 2013 Accepted: 25 June 2013
Published: 9 July 2013

References

1. G Ganesan, Y Li, Cooperative spectrum sensing in cognitive radio - part II: multiuser networks. IEEE Trans Wireless Commun. **6**, 2214–2222 (2007)
2. Y Wei, FR Yu, M Song, Distributed optimal relay selection in wireless cooperative networks with finite-state Markov channels. IEEE Trans Veh. Tech. **59**, 2149–2158 (2010)
3. Q Guan, FR Yu, S Jiang, V Leung, Capacity-optimized topology control for MANETs with cooperative communications. IEEE Trans Wireless Commun. **10**, 2162–2170 (2011)
4. Q Guan, FR Yu, S Jiang, VCM Leung, H Mehrvar, Topology control in mobile ad hoc networks with cooperative communications. IEEE Wireless Comm. **19**, 74–79 (2012)
5. C Hoymann, W Chen, J Montojo, A Golitschek, C Koutsimanis, X Shen, Relaying operation in 3GPP LTE: challenges and solutions. IEEE Comm. Mag. **50**, 156–162 (2012)
6. A Scaglione, D Goeckel, J Laneman, Cooperative communications in mobile ad hoc networks. IEEE Signal Process Mag. **23**, 18–29 (2006)
7. A Gueye, A game theoretical approach to communication security, PhD thesis. University of California at Berkeley (2011)
8. T Basar, GJ Olsder, *Dynamic Noncooperative Game Theory (Classics in Applied Mathematics)*, 2nd edn (Society for Industrial and Applied Mathematics, Philadelphia, 1999)
9. R Ramamoorthy, FR Yu, H Tang, P Mason, A Boukerche, Joint authentication and quality of service design in cooperative communication networks. Comput. Comm. **35**(5), 597–607 (2012)
10. T Heer, S Gotz, OG Morchon, K Wehrle, ALPHA: an adaptive and lightweight protocol for hop-by-hop authentication, in *Proceedings of the 2008 ACM CoNEXT Conference, Madrid, 9–12 December 2008* (ACM, New York, 2008), pp. 1–23
11. J Jiang, JS Thompson, H Sun, A singular-value-based adaptive modulation cooperation scheme for virtual-MIMO systems. IEEE Trans. Veh. Tech. **60**(6), 2495–2504 (2011)
12. J Jiang, JS Thompson, H Sun, PM Grant, Performance assessment of virtual multiple-input multiple-output systems with compress-and-forward cooperation. IET Commun. **6**(11), 1456–1465 (2012)
13. A Nosratinia, TE Hunter, A Hedayat, Cooperative communication in wireless networks. IEEE Commun. Mag. **42**(10), 74–80 (2004)
14. A Bletsas, H Shin, MZ Win, Cooperative communications with outage-optimal opportunistic relaying. IEEE Trans, Wireless Commun. **6**(9), 3450–3460 (2007)
15. A Bletsas, H Shin, MZ Win, Cooperative diversity with opportunistic relaying, in *Proceedings of IEEE WCNC06, Las Vegas, 3–6 April 2006* (IEEE, Piscataway, 2006), pp. 1034–1039
16. K Woradit, T Quek, W Suwansantisuk, M Win, L Wuttisittikulkij, H Wymeersch, Outage behavior of selective relaying schemes IEEE Trans. Wireless Commun. **8**, 3890–3895 (2009)
17. J Liu, FR Yu, C-H Lung, H Tang, Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. IEEE Trans, Wireless Commun. **8**(2), 806–815 (2009)
18. S Bu, FR Yu, P Liu, P Manson, H Tang, Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks. IEEE Trans, Veh. Tech. **60**, 1025–1036 (2011)
19. FR Yu, H Tang, P Mason, F Wang, A hierarchical identity based key management scheme in tactical mobile ad hoc networks. IEEE Trans Net. Serv. Manag. **7**, 258–267 (2010)
20. N Aboudagga, MT Refaei, M Eltoweissy, LA Dasilva, JJ Quisquater, Authentication protocols for ad hoc networks: taxonomy and research issues, in *Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks, Montreal, October 2005* (ACM Press, New York, 2005), pp. 96–104
21. A Perrig, R Canetti, JD Tygar, D Song, *The TESLA broadcast authentication protocol,* vol. 5 (RSA Laboratories, Cambridge, 2002)
22. S Zhu, S Xu, S Setia, S Jajodia, LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks, in *23rd International Conference on Distributed Computing Systems Workshops, Providence, 19–22 May 2003* (IEEE, Piscataway, 2003), pp. 749–749
23. R Akbani, T Korkmaz, GVS Raju, HEAP: a packet authentication scheme for mobile ad hoc networks. Ad Hoc Netw. **6**, 1134–1150 (2008)
24. C Zouridaki, BL Mark, M Hejmo, A quantitative trust establishment framework for reliable data packet delivery in MANETs, in *Proceedings of the Third ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Alexandria, 7–10 November 2005* (ACM, New York, 2005), pp. 1–10
25. S Buchegger, J-YL Boudec, A robust reputation system for mobile ad-hoc networks. Proceedings of P2PEcon. 2003
26. EW Dijkstra, Recursive programming. Numerische Mathematik. **2**, 312–318 (1960)
27. P Paruchuri, JP Pearce, J Marecki, M Tambe, F Ordonez, S Kraus, Playing games for security: an efficient exact algorithm for solving Bayesian Stackelberg games, in *7th international joint conference on Autonomous agents and multiagent systems* (Estoril, Portugal, 12–16 May 2008), pp. 895-902
28. R Ramamoorthy, FR Yu, H Tang, P Mason, Combined authentication and quality of service in cooperative comunication networks, in *2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), Hong Kong, 11–13 December 2010* (IEEE, Piscataway, 2010), pp. 566–571
29. MZ Win, S Member, JH Winters, Virtual branch analysis of symbol error probability for hybrid selection/maximal-ratio combining in Rayleigh fading. IEEE Trans. Commun. **49**, 1926–1934 (2001)
30. P Herhold, E Zimmermann, G Fettweis, A simple cooperative extension to wireless relaying, in *International Zurich Seminar on Communications (IZS)* (IEEE, Piscataway, 2004), pp. 36–39
31. JG Kim, M Krunz, Delay Analysis of Selective Repeat ARQ for a Markovian Source Over a Wireless Channel. IEEE Trans. Veh. Technol. **49**, 1968–1981 (1999)
32. JF Kurose, KW Ross, *Computer Networking: A Top-Down Approach*, 4th edn (Addison Wesley, Boston, 2007)
33. H Liu, H Ma, ME Zarki, S Gupta, Error control schemes for networks: an overview. Mob. Netw. Appl. **2**, 167–182 (1997)
34. S Lin, D Costello, M Miller, Automatic-repeat-request error-control schemes. IEEE Commun. Mag. **22**(12), 5–17 (1984)
35. Y Liu, C Comaniciu, H Man, A Bayesian game approach for intrusion detection in wireless ad hoc networks, in *Proceedings of the Workshop on Game Theory for Communications and Networks 2006 (GameNets '06)* (ACM, New York, 2006)

doi:10.1186/1687-1499-2013-188
Cite this article as: Yu *et al.*: Security and quality of service (QoS) co-design in cooperative mobile *ad hoc* networks. *EURASIP Journal on Wireless Communications and Networking* 2013 **2013**:188.