A Belief Evaluation Framework in Autonomous MANETs under Noisy and Imperfect Observation: Vulnerability Analysis and Cooperation Enforcement

Zhu Ji, Wei Yu, and K.J. Ray Liu, *Fellow, IEEE*

Abstract—In autonomous mobile ad hoc networks (MANETs) where each user is its own authority, the issue of cooperation enforcement must be solved first to enable networking functionalities such as packet forwarding, which becomes very difficult under noisy and imperfect monitoring. In this paper, we consider cooperation enforcement in autonomous mobile ad hoc networks under noisy and imperfect observation and study the basic packet forwarding among users through the repeated game models with imperfect information. A belief evaluation framework is proposed to obtain cooperation-enforcement packet forwarding strategies only based on each node's private information including its own past actions and imperfect observation of other nodes' information. More importantly, we not only show that the proposed strategy with belief system can maintain the cooperation paradigm but also establish its performance bounds. The simulation results illustrate that the proposed belief evaluation framework can enforce the cooperation with only a small performance degradation compared with the unconditionally cooperative outcomes when noisy and imperfect observation exist.

Index Terms—Belief evaluation, MANETs, cooperation enforcement, game theory.

1 Introduction

Mobile ad hoc networks (MANETs) have drawn extensive attention in recent years due to the increasing demands of their potential applications [1], [2]. In traditional crisis or military situations, the nodes in a MANET usually belong to the same authority and work in a fully cooperative way of unconditionally forwarding packets for each other to achieve their common goals. Recently, the MANETs are also envisioned to be deployed for civilian applications [3], [4], [5], [6], [7], [8], [9], where nodes typically do not belong to a single authority and may not pursue a common goal. Consequently, fully cooperative behaviors cannot be directly assumed, as the nodes are selfish to maximize their own interests. We refer to such networks as autonomous (or self-organized) MANETs.

However, before ad hoc networks can be successfully deployed in an autonomous way, the issue of cooperation enforcement must be resolved first. One way to enforce cooperation among selfish nodes is to use payment-based schemes, such as [6], [8], in which a selfish node will forward packets for other nodes only if it can get some payment from those requesters as compensation. Another way to enforce cooperation among selfish nodes is to use reputation-based schemes with necessary traffic monitoring mechanisms, such as [3], [4], [5], [7], [10], in which a node determines whether it should forward packets for other nodes or request other nodes to forward packets for it based on their past behaviors. In [3], a reputation-based system was proposed for ad hoc networks to mitigate nodes' misbehaviors, where each node launches a "watchdog" to monitor its neighbors' packet forwarding activities. Following [3], CORE and CONFIDANT systems [4], [5] were proposed to enforce cooperation among selfish nodes which aim at detecting and isolating misbehaving node and thus making it unattractive to deny cooperation. Moreover, ARCS was proposed in [7] to further defend against various attacks while providing the incentives for cooperation.

Recently, some efforts have been made toward mathematical analysis of cooperation in autonomous ad hoc networks using game theory, such as [9], [11], [12], [13], [14]. In [9], Srinivasan et al. provided a mathematical framework for cooperation in ad hoc networks, which focuses on the energy-efficient aspects of cooperation. In [11], Michiardi and Molva studied the cooperation among selfish nodes in a cooperative game theoretic framework. In [12], Altman et al. studied the packet forwarding problem using a noncooperative game theoretic framework. Further, Trust modeling and evaluation framework [15], [16] have been extensively studied to enhance cooperation in autonomous distributed networks, which utilized trust (or belief) metrics to assist decision making in autonomous networks through trust recommendation and propagation. In [13], [14], the reputation frameworks based on Bayesian formulation were proposed to increase the integrity and cooperation of wireless ad hoc or sensor networks.

- *Z. Ji is with Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121. E-mail: zji@qualcomm.com.*
- *W. Yu is with Microsoft Corporation, One Microsoft Way, Redmond, WA 98052. E-mail: weiy@microsoft.com.*
- *K.J.R. Liu is with the Department of Electrical and Computer Engineering and the Institute for Systems Research, University of Maryland, 2232 Kim Building, College Park, MD 20742. E-mail: kjrliu@umd.edu.*

Manuscript received 6 Feb. 2009; revised 9 Oct. 2009; accepted 3 Dec. 2009; published online 28 Apr. 2010.
For information on obtaining reprints of this article, please send e-mail to: tmc@computer.org, and reference IEEECS Log Number TMC-2009-02-0042.
Digital Object Identifier no. 10.1109/TMC.2010.87.

1536-1233/10/$26.00 © 2010 IEEE Published by the IEEE CS, CASS, ComSoc, IES, & SPS

One major drawback of these existing game theoretic analyses on cooperation in autonomous ad hoc networks lies in that all of them have assumed perfect observation. However, in autonomous ad hoc networks, even when a node has decided to forward a packet for another node, this packet may still be dropped due to link breakage or transmission errors. Further, since central monitoring is, in general, not available in autonomous ad hoc networks, perfect public observation is either impossible or too expensive. Therefore, how to stimulate cooperation and analyze the efficiency of possible strategies in the scenarios with noisy and imperfect observation is still unanswered in autonomous ad hoc networks.

In this paper, we study the cooperation enforcement for autonomous mobile ad hoc networks under noisy and imperfect observation and focus on the most basic networking functionality, namely packet forwarding. Considering the nodes need to infer the future actions of other nodes based on their own imperfect observations, in order to optimally quantify the inference process with noisy and imperfect observation, a belief evaluation framework is proposed to stimulate the packet forwarding between nodes and maximize the expected payoff of each selfish node by using repeated game theoretical analysis. Specifically, a formal belief system using Bayes' rule is developed to assign and update beliefs of other nodes' continuation strategies for each node based on its private imperfect information. Further, we not only show that the packet forwarding strategy obtained from the proposed belief evaluation framework achieves a sequential equilibrium [17] that guarantees the strategy to be cheat-proof but also derive its performance bounds. The simulation results illustrate that the proposed packet forwarding approach can enforce the cooperation in autonomous ad hoc networks under noisy and imperfect observation with only a small performance degradation compared to the unconditionally cooperative outcomes.

The rest of this paper is organized as follows: In Section 2, we illustrate the system model of autonomous ad hoc networks under noisy and imperfect observation and derive corresponding game theoretical formulation. Vulnerability analysis for autonomous MANETs under noisy and imperfect observation is carried out in Section 3. In Section 4, we propose the belief evaluation framework and carry out the equilibrium and efficiency analysis for one-hop and multinode multihop packet forwarding. The simulation studies are provided in Section 5. Finally, Section 6 concludes this paper.

2 System Model and Game Theoretical Formulation

2.1 System Model

We consider autonomous ad hoc networks where nodes belong to different authorities and have different goals. Assume all nodes are selfish and rational, that is, their objectives are to maximize their own payoff, not to cause damage to other nodes. Each node may act as a service provider, scheduling packets to be generated and delivered to certain destinations, or act as a relay, forwarding packets for other nodes. The sender will get some payoffs if the packets are successfully delivered to the destination and the forwarding effort of relay nodes will also introduce certain costs.

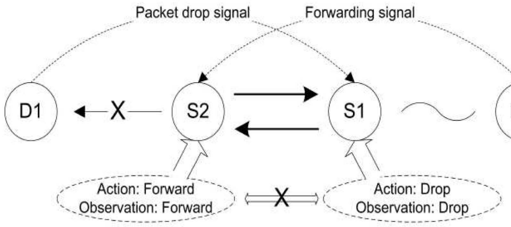


Fig. 1. Packet forwarding in autonomous ad hoc networks under noisy and imperfect observation.

In this paper, we assume that some necessary traffic monitoring mechanisms, such as those described in [3], [6], [7], will be launched by each node to keep tracking of its neighbors' actions. However, it is worth mentioning that we do not assume any public or perfect observation, where a public observation means that when an action happens, a group of nodes in the network will have the same observation, and perfect observation means all actions can be perfectly observed without any mistake. In ad hoc networks, due to its multihop nature and the lack of central monitoring mechanism, public observation is usually not possible. Meanwhile, to our best knowledge, there exist no such monitoring mechanisms in ad hoc networks that can achieve perfect observation. Instead, in this paper, we study the cooperation-enforcement strategies based on imperfect private observation. Here, private means that the observation of each node is only known to itself and won't or cannot be revealed to others.

We focus on two scenarios causing imperfect observation in ad hoc networks. One scenario is that the outcome of a forwarding action maybe a packet-drop due to link breakage or transmission errors. The other scenario is that a node has dropped a packet but is observed as forwarding the packet, which may happen when the watchdog mechanism [3] is used and the node wants to cheat its previous node on the route. Fig. 1 illustrates our system model by showing a network snapshot of one-hop packet forwarding between two users at a certain time stage under noisy and imperfect observation. In this figure, there are two source-destination pairs (S_1, D_1) and (S_2, D_2). S_1 and S_2 need to help each other to forward packets to the destination nodes. At this stage, node S_1 drops the packet and observes the packet-drop signal of node S_2's action, while node S_2 forwards the packet and observes the forwarding signal of node S_1's action. The action and observation of each node are only known to itself and cannot or will not be revealed to other nodes. Due to transmission errors or link breakage between S_2 and D_1, S_2's forwarding action is observed as a packet-drop signal; due to possible cheating behavior between S_1 and D_2, a forfeit forwarding signal maybe observed by S_2. Therefore, it is important to design strategies for each node to make the optimal decision solely based on these imperfect private information.

2.2 Static and Repeated Packet Forwarding Game Model

We model the process of routing and packet forwarding between two nodes forwarding packets for each other as a game. The players of the game are two network nodes, denoted by $i \in I = \{1, 2\}$. Each player is able to serve as the relay for the other player and needs the other player to forward packets for him based on current routing selection and topology. Each player chooses his action, i.e., strategy, a_i from the action set $A = \{F, D\}$, where F and D are packet forwarding and dropping actions, respectively. Also, each player observes a private signal ω of the opponent's action from the set $\Omega = \{f, d\}$, where f and d are the observations of packet forwarding and dropping signals, respectively. Since the player's observation cannot be perfect, the forwarding action F of one player maybe observed as d by the other player due to link breakage or transmission errors. We let such probability be p_f. Also, the noncooperation action D maybe observed as the cooperation signal f under certain circumstances. Without loss of generality, let the observation error probability be p_e in our system, which is usually caused by malicious cheating behaviors and indicates that the group of packets is actually dropped though forwarding signal f is observed. For instance, if the destination node is colluding with the relay node, it can send back an acknowledgment even if it doesn't receive the packets. Another scenario in which $p_e > 0$ is that if there is dedicated control channel between the source and destination that is different from data channel and only responsible for sending feedback, the physical channel errors may cause the NACK message to be decoded as ACK message. For each node, the cost of forwarding a group of packets for the other node during one stage of play is ℓ, and the gain it can get for the packets that the other node has forwarded for it is $\tilde{g}$. Usually, the gain of successful transmission is for both the source and destination nodes. Noting that the source and destination pair in ad hoc networks usually serves for a common communication goal, we consider the gain goes to the source for the game modeling without loss of generality.

We first consider the packet forwarding as a static game [18], which is only played once. Given any action profile $a = (a_1, a_2)$, we refer to $u(a) = (u_1(a), u_2(a))$ as the expected payoff profile. Let a_{-i} and $\mathrm{Prob}(\omega_i|a_{-i})$ be the action of the ith player's opponent and the probability of observation ω_i given a_{-i}, respectively. Then, $u_i(a)$ can be obtained as follows:

$$u_i(a) = \sum_{\omega_i \in \Omega} \tilde{u}_i(a_i, \omega_i, a_{-i}) \cdot \mathrm{Prob}(\omega_i|a_{-i}), \tag{1}$$

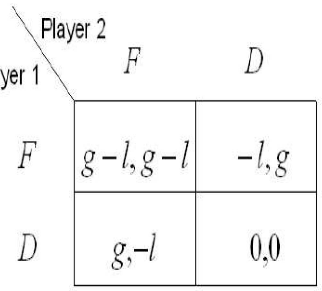
where $\tilde{u}_i$ is the ith player's payoff determined by the action profile and his own observation. Then, calculating $u(a)$ for different strategy pairs, we have the strategic form of the static packet forwarding game as a matrix in Fig. 2. Note that $g = (1 - p_f) \cdot \tilde{g}$, which can be obtained from (1) considering the possibility of the packet-drop.

To analyze the outcome of a static game, the Nash Equilibrium [17], [18] is a well-known concept, which is a set of strategies, one for each player, such that no selfish player has incentive to unilaterally change his/her action. Noting that our two-player packet forwarding game is similar to the setting of the prisoner's dilemma game, the only Nash equilibrium is the action profile $a^* = (D, D)$, and the better cooperation payoff outcome $(g - \ell, g - \ell)$ of the cooperation action profile $\{F, F\}$ cannot be practically realized in the static packet forwarding game due to the greediness of the players. However, generally speaking, the above packet forwarding game will be played many times in real ad hoc networks. It is natural to extend the above static game model to a multistage game model [18]. Considering that the past packet forwarding behaviors do not influence the feasible actions or payoff function at current stage, the multistage packet forwarding game can be further analyzed using the repeated game model [17], [18]. Basically, in the repeated games, the players face the same static game at every period, and the player's overall payoff is a weighted average of the payoffs at each stage over time. Let ω_i^t be the privately observed signal of the ith player in period t. Suppose that the game begins in period 0 with the null history h^0. In this game, a private history for player i at period t, denoted by h_i^t, is a sequence of player i's past actions and signals, i.e., $h_i^t = \{a_i^\tau, \omega_i^\tau\}_{\tau=1}^{t-1}$. Let $H_i^t = (A \times \Omega)^t$ be the set of all possible period-t histories for the ith player. Denote the infinite packet forwarding repeated game with imperfect private histories by $G(p, \delta)$, where $\delta \in (0, 1)$ is the discount factor and $p = (p_f, p_e)$. Assume that $p_f < 1/2$ and $p_e < 1/2$. Then, the overall discounted payoff for player $i \in I$ is defined as follows [18]:

$$U_i(\delta) = (1 - \delta) \sum_{t=0}^{\infty} \delta^t u_i^t\big(a_1^t\big(h_1^t\big), a_2^t\big(h_2^t\big)\big). \tag{2}$$

Folk Theorems for infinite repeated games [18] assert that there exists $\hat{\delta} < 1$ such that any feasible and individually rational payoff can be enforced by an equilibrium for all $\delta \in (\hat{\delta}, 1)$ based on the public information shared by players. However, one crucial assumption for the Folk Theorems is that players share common information about each other's actions. In contrast, the nature of our repeated packet forwarding game for autonomous ad hoc networks determines that the nodes' behavioral strategies can only rely on the private information histories including their own past actions and imperfectly observed signals.

Such a minor game-setting change from the public observation to the private observation due to noisy and imperfect observation will make a substantial difference in analyzing the efficiency of the packet forwarding game. In the situation of imperfect private observation, no recursive structure [19] exists for the forwarding strategies since the player decides their actions according to various private histories. Each node must conduct statistical inference to detect potential deviations and estimate what others are going to do next, which can become extremely complex due to the imperfect observation [20], [21].



Player 1 \ Player 2	F	D
F	g − l, g − l	−l, g
D	g, −l	0,0

Fig. 2. Two-player packet forwarding game in strategic form.

3 Vulnerability Analysis

In this section, we analyze the vulnerability caused by noisy and imperfect observation in autonomous MANETs. First, we study the system vulnerability in the scenario of one-hop packet forwarding. Then, we further exploit the effect of noisy and imperfect observation in the scenario of multihop packet forwarding.

In the scenario of one-hop packet forwarding, the interactions between a pair of nodes forwarding packets for each other can be modeled as the two-player game in the previous section. Although it is seemingly a minor game-setting change from the public observation to the private observation due to noisy and imperfect observation, such change on game-setting introduces substantial challenges on the interactions, outcomes, and efficiency of our packet forwarding game, which can be illustrated as follows: First, the observation errors caused by the noisy and imperfect observation indicate that simple TIT-for-TAT [12], [22] strategies are not able to enforce efficient cooperation paradigm among users since such equivalent retaliation strategy leads to inefficient noncooperative outcomes. Second, considering the selfishness of the users along with the effects of noisy and imperfect observations, the users won't share their action information or observations of others' actions, which indicates that no public information available for the users. Therefore, the users are not able to coordinate their strategies for efficient outcomes relying only on private histories, i.e., no recursive structure [19] exists for the forwarding strategies since the players decide their actions according to various private histories. Third, although the dynamic game theory has studied and defined the equilibrium concepts on the outcomes of the game with imperfect information, such as Sequential Equilibrium (SE) [17], [18] or Perfect Bayesian Equilibrium (PBE) [17], [18], it doesn't provide generalized efficient mechanisms to achieve SE or PBE in the scenarios of private information. Note that generous tit-for-tat (GTFT) [9], [22], [23] is able to partly alleviate the impact of noisy and imperfect observation on the efficiency of the packet forwarding game outcomes by assuming that the nodes may be generous to contribute more to the network than to benefit from it. However, GTFT is lack off of a formalized structure of the belief definition and belief updating. It is difficult to extend GTFT to the multiplayer game scenarios that need user coalition to achieve cooperation and improve the efficiency such as the multihop multinode MANETs. Also, the existing GTFT research doesn't consider the observation error p_e defined in Section 2.

Based on the above discussions, the noisy and imperfect observation causes several vulnerability issues even for simple one-hop packet forwarding in autonomous MANETs, which can be illustrated as follows:

- Since the nodes make decisions based on private information, each node must conduct statistical inference to detect potential deviations and estimate what others are going to do next. The constraint of the noisy and imperfect observation will result in false alarms or detection errors. Selfish nodes maybe able to utilize such fact to contribute fewer efforts while getting more benefits from others.
- Considering that the nodes are not willing to or not able to share their information, the nodes cannot rely on others' past experiences or recommendations on the nodes' behaviors, which gives the selfish nodes more flexibility on their cheating behaviors.
- Due to the observation errors, the cooperative nodes may falsely accuse other cooperative nodes of seemingly noncooperative behaviors, which is actually caused by link breakage or transmission errors. How to maintain the cooperative paradigm in such scenarios remains a challenging problem.

In the scenario of multinode and multihop packet forwarding, more sophisticated vulnerability issues will be raised considering the challenges of the self-organizing routing and the correlation of the nodes' actions. In general, due to the multihop nature, when a node wants to send a packet to a certain destination, a sequence of nodes need to be requested to help forwarding this packet. We refer to the sequence of (ordered) nodes as a route, the intermediate nodes on a route as relay nodes, and the procedure to discover a route as route discovery. In general, the routing process includes route discovery and packet forwarding. The route discovery carries out three steps consecutively. First, the requester notifies the other nodes in the network that it wants to find a route to a certain destination. Second, other nodes in the network will make their decisions on whether agreeing to be on the discovered route or not. Third, the requester will determine which route should be used. Based on the discussion of the routing process, we can see that the action and observation of one node on a route will largely affect the behaviors of other nodes on this route or alternative routes between the source and destination nodes, which in reverse affects the behavior of the original node. The above properties of multinode and multihop packet forwarding may introduce more vulnerability issues than one-hop packet forwarding illustrated as follows:

- In the scenarios of multiple nodes on one route, it becomes very difficult to detect the users with cheating behaviors only based on the private and incomplete local information available to each node.
- Since the routing process involves different steps, the seemingly cooperative behaviors at each stage may jointly have cheating effects across multiple steps. From the game theoretical point of view, each stage game in our dynamic packet forwarding game consists of several subgames, such as route participation subgame or route selection subgame. The vulnerability issues need to be considered not only for each subgame but also for the overall game.
- The multihop routing makes the observation of nodes more difficult as the packet-drop action at one node will affect the outcome of the multihop routing. Such propagation effects can be taken advantage of by selfish nodes to cheat for more payoffs.

In order to combat the above vulnerability issues on autonomous MANETs under noisy and imperfect observation, it is important to study novel strategy framework comprehensively considering these issues.

4 A Belief Evaluation Framework

In this section, we first develop a belief evaluation framework for two-player packet forwarding game in attempt to shed light on the solutions to the more complicated multiplayer case. Efficiency study is then carried out to analyze the equilibrium properties and performance bounds. Further, a belief evaluation framework is proposed for general networking scenarios with multiple nodes and multihop routing.

4.1 Two-Player Belief-Based Packet Forwarding

In order to have an efficient and robust forwarding strategy based on each node's own imperfect observation and actions, enlightened by [21], we propose a belief evaluation framework to enforce cooperation.

First, we define two strategies, i.e., σ_F and σ_D. Let σ_F be the trigger cooperation strategy, which means that the player forwards packets at current stage, and at the next stage, the player will continue to forward packets only if it observes the other player's forwarding signal f. Let σ_D be the defection strategy, which means that the player always drops packets regardless of its observation history. Such strategies are also called continuation strategies [21]. Since both of the two strategies also determine the player's following actions at every private history, the strategy path and expected future payoffs caused by any pair of the two strategies are fully specified. Let $V_{\alpha,\beta}(p,\delta), \alpha, \beta \in \{F, D\}$ denote the repeated game payoff of σ_α against σ_β, which can be illustrated by the following Bellman equations [24] for different pairs of continuation strategies:

$$\begin{aligned} V_{FF} &= (1-\delta)(g-\ell) + \delta\big((1-p_f)^2 V_{FF} \\ &\quad + p_f(1-p_f)V_{FD} + p_f(1-p_f)V_{DF} + p_f^2 \cdot V_{DD}\big), \quad (3) \\ V_{FD} &= -(1-\delta)\ell + \delta((1-p_f)(1-p_e)V_{DD} \\ &\quad + p_f(1-p_e)V_{DD} + p_e(1-p_f)V_{FD} + p_f p_e V_{FD}), \quad (4) \\ V_{DF} &= (1-\delta)g + \delta((1-p_f)(1-p_e)V_{DD} \\ &\quad + p_e(1-p_f)V_{DF} + p_f(1-p_e)V_{DD} + p_e p_f V_{DF}), \quad (5) \\ V_{DD} &= (1-\delta)\cdot 0 + \delta\big((1-p_e)^2 V_{DD} + \\ &\quad p_e(1-p_e)V_{DD} + p_e(1-p_e)V_{DD} + p_e^2 \cdot V_{DD}\big). \quad (6) \end{aligned}$$

Generally speaking, a Bellman equation [24] breaks a dynamic optimization problem into simpler subproblems, representing the payoff of a dynamic programming problem at a certain point in time in terms of the payoff from some initial choices at this time point and the payoff of the future time period that results from those initial choices. Note that the first terms on the right-hand side (RHS) of (3)-(6) represent the normalized payoffs of current period with specific initial choices of $\{\alpha, \beta\}$, while the second terms illustrate the expected continuation payoffs considering four possible outcomes due to the noisy and imperfect observation.

By solving the above equations, $V_{\alpha,\beta}(p,\delta)$ can be easily obtained. Then, we have $V_{DD} > V_{FD}$, for any δ, p. Furthermore, if $\delta > \delta_0$, then $V_{FF} > V_{DF}$, where δ_0 can be obtained as

$$\delta_0 = \frac{\ell}{(1-p_f-p_e)g - [p_f(1-p_f) - p_e]\ell}. \quad (7)$$

Intuitively, V_{FF} needs to be greater than V_{DF} so that the cooperative behaviors introduce greater overall payoff. Then, it is possible to enforce the cooperation behavior among the selfish users since V_{FF} dominates V_{DF} in the long run. Therefore, it is important to constrain $\delta > \delta_0$ in our study.

TABLE 1
Two-Player Packet Forwarding Algorithm

1. Initialize using system parameter configuration (δ, p_e, p_f)**:** Node i initializes his belief μ_i^1 of the other node as $\pi(\delta, p)$ and chooses the forwarding action in period 1.
2. Belief update based on the private history: Update each node's belief μ_i^{t-1} into μ_i^t using (10-13) according to different realizations of private history.
3. Optimal Decision of the player's next move: If the continuation belief $\mu_i^t > \pi$, node i plays σ_F; If the continuation belief $\mu_i^t < \pi$, node i plays σ_D; If the continuation belief $\mu_i^t = \pi$, node i plays either σ_F or σ_D.
4. Iteration: Let $t = t + 1$, then go back to Step 2.

Suppose that player i believes that his opponent is playing either σ_F or σ_D, and is playing σ_F with probability μ. Then, the difference between his payoff of playing σ_F and the payoff of playing σ_D is given by

$$\triangle V(\mu; \delta, p) = \mu \cdot (V_{FF} - V_{DF}) - (1-\mu) \cdot (V_{DD} - V_{FD}). \quad (8)$$

Hence, $\triangle V(\mu)$ is increasing and linear in μ and there is a unique value $\pi(p, \delta)$ to make it zero, which can be obtained as follows:

$$\pi(\delta, p) = \frac{-V_{FD}(\delta, p)}{V_{FF}(\delta, p) - V_{DF}(\delta, p) - V_{FD}(\delta, p)}, \quad (9)$$

where $\pi(p, \delta)$ is defined so that there is no difference for player i to play σ_F or σ_D when player j plays σ_F with probability $\pi(\delta, p)$ and σ_D with probability $1 - \pi(\delta, p)$. For simplicity, $\pi(\delta, p)$ maybe denoted as π under the circumstances with no confusion. In general, if node i holds the belief that the other node will help him to forward the packets with a probability smaller than $1/2$, node i is inclined not to forward packets for the other node. Considering such situation, we let δ be such that $\pi(\delta, p) > 1/2$.

It is worth mentioning that (8) is applicable to any period. Thus, if a node's belief of an opponent's continuation strategy being σ_F is μ, in order to maximize its expected continuation payoff, the node prefers σ_F to σ_D if $\mu > \pi$ and prefers σ_D to σ_F if $\mu < \pi$. Starting with any initial belief μ, the ith player's new belief when he takes action a_i and receives signal ω_i can be defined using Bayes' rule [18] as follows:

$$\mu\big(h_i^{t-1}, (F, f)\big) = \frac{\mu(h_i^{t-1})(1-p_f)^2}{\mu(h_i^{t-1})(1-p_f) + p_e \cdot (1 - \mu(h_i^{t-1}))}, \quad (10)$$

$$\mu\big(h_i^{t-1}, (F, d)\big) = \frac{\mu(h_i^{t-1})(1-p_f) \cdot p_f}{\mu(h_i^{t-1}) \cdot p_f + (1-p_e) \cdot (1 - \mu(h_i^{t-1}))}, \quad (11)$$

$$\mu\big(h_i^{t-1}, (D, f)\big) = \frac{\mu(h_i^{t-1})(1-p_f) \cdot p_e}{\mu(h_i^{t-1}) \cdot (1-p_f) + p_e \cdot (1 - \mu(h_i^{t-1}))}, \quad (12)$$

$$\mu\big(h_i^{t-1}, (D, d)\big) = \frac{\mu(h_i^{t-1}) p_f \cdot p_e}{\mu(h_i^{t-1}) \cdot p_f + (1-p_e) \cdot (1 - \mu(h_i^{t-1}))}. \quad (13)$$

From on the above discussion, we propose a two-player packet forwarding algorithm based on the developed belief evaluation framework in Table 1. Note that by using the proposed belief system, each node only needs to maintain its belief value, its most recent observation and action instead of the long-run history information of interactions with other users.

4.2 Efficiency Analysis

In this part, we show that the behaviorial strategy obtained from the proposed algorithm with well-defined belief system is a sequential equilibrium [17] and further analyze its performance bounds.

First, we briefly introduce the equilibrium concepts of the repeated games with imperfect information. As for the infinitely repeated game with perfect information, the Nash Equilibrium concept is a useful concept for analyzing the game outcomes. Further, in the same scenario with perfect information, **Subgame Perfect Equilibrium** (SPE) [17] can be used to study the game outcomes, which is an equilibrium such that users' strategies constitute a Nash equilibrium in every subgame [18] of the original game, which eliminate those Nash Equilibria in which the players' threats are incredible. However, the above equilibrium criteria for the infinitely repeated game require that perfect information can be obtained for each player. In our packet forwarding game, each node is only able to have its own strategy history and form the beliefs of other nodes' future actions through imperfect observation. **Sequential Equilibrium** [17] is a well-defined counterpart of subgame perfect equilibrium for multistage games with imperfect information, which has not only sequential rationality that guarantees that any deviations will be unprofitable but also consistency on zero-probability histories.

In our packet forwarding game with private history and observation, the proposed strategy with belief system can be denoted as (σ^*, μ), where $\mu = \{\mu_i\}_{i\in I}$ and $\sigma^* = \{\sigma_i^*\}_{i\in I}$. By studying (10), we find that there exists a point ϕ such that $\mu(h_i^{t-1},(F,f)) < \mu(h_i^{t-1})$ as $\mu(h_i^{t-1}) > \phi$ while $\mu(h_i^{t-1},(F,f)) > \mu(h_i^{t-1})$ as $\mu(h_i^{t-1}) < \phi$. Here, ϕ can be calculated as $\phi = [(1-p_f)^2 - p_e]/(1-p_f-p_e)$. It is easy to show that $\mu(h_i^{t-1},(a_i,\omega_i)) < \mu(h_i^{t-1})$ when (F,d), (D,f), and (D,d) are reached. Since we initialize the belief with π we have $\mu_i^t \leq \phi$ after any belief-updating operation if $\pi < \phi$. Considering the belief updating in the scenario that $\pi \geq \phi$ becomes trivial, we assume $\pi < \phi$ thus $\mu_i^t \in [0,\phi]$ and $\phi \geq 1/2$. Then, let the proposed packet forwarding strategy profile σ^* be defined as: $\sigma_i^*(\mu_i) = \sigma_F$ if $\mu_i > \pi$ and $\sigma_i^*(\mu_i) = \sigma_D$ if $\mu_i < \pi$; if $\mu_i = \pi$, the node forwards packets with probability π and drops them with probability $1-\pi$. Noting that $\pi(\delta, p) \leq \phi$, we obtain another constraint on δ, which can be written as follows:

$$\delta \geq \underline{\delta} = \frac{\ell}{[(1-p_f)^2 - p_e]\cdot g + \ell \cdot p_e}. \tag{14}$$

Using the above equilibrium criteria for the repeated games with imperfect information, we then analyze the properties of the proposed strategy illustrated in Table 1 through the following theorems.

Theorem 1. *The proposed strategy profile σ^* with belief system μ from Table 1 is a sequential equilibrium for $\pi \in (1/2, \phi)$.*

Proof. See the Appendix. □

Theorem 1 shows that the strategy profile σ^* and the belief system μ obtained from the proposed algorithm is a sequential equilibrium, which not only responds optimally at every history but also has consistency on zero-probability histories. Thus, the cooperation can be enforced using our proposed algorithm since the deviation will not increase the players' payoffs. Then, similar to [21], it is straightforward to prove the following theorem, which addresses the efficiency of the equilibrium and shows that when the p_e and p_f are small enough, our proposed strategy approaches the cooperative payoff $g - \ell$.

Theorem 2. *Given g and ℓ, there exist $\tilde{\delta} \in (0,1)$ and $\tilde{p}$ for any small positive τ such that the average payoff of the proposed strategy σ^* in the packet forwarding repeated game $G(p,\delta)$ is greater than $g - \ell - \tau$ if $\delta > \tilde{\delta}$ and $p_e, p_f < \tilde{p}$.*

However, in real ad hoc networks, considering the mobility of the node, channel fading, and the cheating behaviors of the nodes, it may be not practical to assume very small p_e and p_f values. A more useful and important measurement is the performance bounds of the proposed strategy given some fixed p_e and p_f values. We further develop the following theorem studying the lower bound and upper bound of our strategy to provide a performance guideline. In order to model the prevalent data application in current ad hoc networks, we assume the game discount factor is very close to 1.

Theorem 3. *Given the fixed (p_e, p_f) and discount factor of the repeated game δ_G close to 1, the payoff of the proposed algorithm in Table 1 is upper bounded by*

$$\bar{U} = (1-\kappa)\cdot(g-\ell), \tag{15}$$

where

$$\kappa = \frac{p_f \cdot [g(1-p_f) + \ell]}{(1-p_f-p_e)(g-\ell)}. \tag{16}$$

The lower bound of the performance will approach the upper bound when the discount factor of the repeated game δ_G approaches 1 and the packet forwarding game is divided into N subgames as follows: the first subgame is played in period $1, N+1, 2N+1, \ldots$ and the second subgame is played in period $2, N+2, 2N+2, \ldots$, and so on. The optimal N is

$$N = \lfloor \log \underline{\delta} / \log \delta_G \rfloor, \tag{17}$$

The proposed strategy is played in each subgame with equivalent discount factor δ_G^N.

Proof. By substituting $V_{\alpha,\beta}$ obtained from (3)-(6) into (9), we have

$$\pi(\delta, p) = \frac{\ell}{g-\ell}\cdot\frac{1-\delta(1-p_f)^2}{\delta(1-p_f-p_e)}. \tag{18}$$

Then, since the node i is indifferent of forwarding or dropping packets if its belief of the other node is equal to π, the expected payoff of the node i at the sequential equilibrium (σ^*, μ) can be written as

$$V(\pi,\delta,p) = \pi(\delta,p)\cdot V_{DF}(\delta,p) + (1-\pi(\delta,p))\cdot V_{DD}(\delta,p). \tag{19}$$

It is easy to show that $V(\pi(\delta,p),\delta,p)$ is a decreasing function in δ when $\delta \in (0,1)$. Then, the upper bound of the expected payoff can be obtained by letting δ be the smallest feasible value. From (7) and (14), we have $\delta > \underline{\delta}$ and $\delta > \delta_0$. Since $\underline{\delta} > \delta_0$, we can derive the upper bound of the payoff of the proposed algorithm as (15) by substituting $\underline{\delta}$ into (19).

However, the discount factor of our game is usually close to 1. Generally, $\underline{\delta}$ is a relatively smaller value in the range of $(0, 1)$. In order to emulate the optimal discount factor $\underline{\delta}$, we introduce the following game partition method. We partition the original repeated game $G(p, \delta_G)$ into N distinct subgames as the theorem illustrates. Each subgame can be regarded as a repeated game with the discount factor δ_G^N. The optimal subgame number N, which minimizes the gap between δ_G^N and $\underline{\delta}$, can be calculated as $N = \lfloor \log \underline{\delta} / \log \delta_G \rfloor$.

As there is always difference between δ_G^N and $\underline{\delta}$, it is more important to study the maximal gap, which results in the lower bound of the payoff using our game partition method. Similar to [25], we can show that by using the optimal N, $\delta_G^N \in [\underline{\delta}, \bar{\delta}]$, where $\bar{\delta} = \underline{\delta}/\delta_G$. Substituting $\bar{\delta}$ into (19), we have the lower bound of the payoff of our proposed algorithm with the proposed game partition method. When δ_G approaches 1, and $\bar{\delta}$ approaches $\underline{\delta}$, the payoff of our algorithm achieves the payoff upper bound. □

In the above theorem, the idea of dividing the original game into some subgames is useful to maintain the efficiency when δ approaches one for our game setting. A larger δ indicates that future payoffs are more important for the total payoff, which results in more number of subgames. Since there are multiple subgames using the belief-based forwarding strategy, even if the outcomes of some subgames become the noncooperation case due to the observation errors, cooperation plays can still continue in other subgames to increase the total payoff. Therefore, compared to the trigger strategy for ad hoc networks [26] in which a node stops cooperating with other nodes if one single defection is observed, our approach is much more robust to the defection caused by noisy and imperfect observation with the above subgame partition approach. Also, our proposed belief system takes into consideration of observation or link errors.

4.3 Multinode Multihop Packet Forwarding

In the previous parts, we mainly focus on the two-player case, while in an ad hoc network there usually exist many nodes and multihop routing is generally enabled. In this section, we model the interactions among selfish nodes in an autonomous ad hoc network as a multiplayer packet forwarding game, and develop the optimal belief evaluation framework based on the two-player belief system.

4.3.1 Multinode Multihop Game Model

In this section, we consider autonomous ad hoc networks where nodes can move freely inside a certain area. For each node, packets are scheduled to be generated and sent to certain destinations. Different from the two-player packet forwarding game, the multiplayer packet forwarding game studies multihop packet forwarding which involves the interactions and beliefs of all the nodes on the route. Before studying the belief-based packet forwarding in this scenario, we first model the multiplayer packet forwarding game as follows:

- There are M players in the game, which represent M nodes in the network. Denote the player set as $I_M = \{1, 2, \ldots, M\}$.
- For each player $i \in I_M$, he has groups of packets to be delivered to certain destinations. The payoff of successfully having a group of packets delivered during one stage is denoted by $\tilde{g}$.
- For each player $i \in I_M$, forwarding a group of packets for another player will incur the cost ℓ.
- Due to the multihop nature of ad hoc networks, the destination player may be not in the sender i's direct transmission range. Player i needs to not only find the possible routes leading to the destination (i.e., route discovery), but also choose an optimal route from multiple routing candidates to help forwarding the packets (i.e., route selection).
- Each player only knows his own past actions and imperfect observation of other players' actions. Note that the information history consisting of the above two parts is private to each player.

Similar to [9], we assume the network operates in discrete time. In each time slot, one node is randomly selected from the M nodes as the sender. The probability that the sender finds r possible routes is given by $q_r(r)$ and the probability that each route needs $\hbar$ hops is given by $q_{\hbar}(\hbar)$ (assume at least one hop is required in each time slot). Note that the $\hbar$ relays on each route are selected from the rest of nodes with equal probability and $\hbar \leq \lfloor \tilde{g}/\ell \rfloor$. Assume each routing session lasts for one slot and the routes remain unchanged within each time slot. In our study, we consider that delicate traffic monitoring mechanisms, such as receipt-submission approaches [6], are in place, hence, the sender is able to have the observation of each node on the forwarding route.

4.3.2 Belief Evaluation System Design

In this part, we develop an efficient belief evaluation framework for multihop packet forwarding games based on the proposed two-player approach. Since a successful packet transmission through a multihop route depends on the actions of all the nodes on the route, the belief evaluation system needs to consider the observation error caused by each node, which makes a direct design of the belief system for the multiplayer case very difficult. However, the belief system derived for two-player scenarios can serve as the baseline of how to derive the beliefs in the scenarios of multihop and multinodes scenarios. Although there are more complicated interactions between nodes and among a group of nodes while forming a multihop forwarding route, the belief of each user are still based on the mutual interactions with other nodes from his/her own observations.

Different from single-hop two-player packet forwarding game, in the multihop multinode packet forwarding, the nodes on each route that are successfully formed can be considered as a coalition [17]. And, the cooperation within a coalition can only be enforced while the players follow certain common game rules. The game also becomes a competition between coalitions of players, rather than individual nodes. Since we study the selfish nodes, proper game rules need to be introduced to maximize the payoff of each user and prevent the unilateral or multilateral deviation from the game strategy depending on what optimization game criteria are applied. Considering the derived belief system for the two-player game leads to a

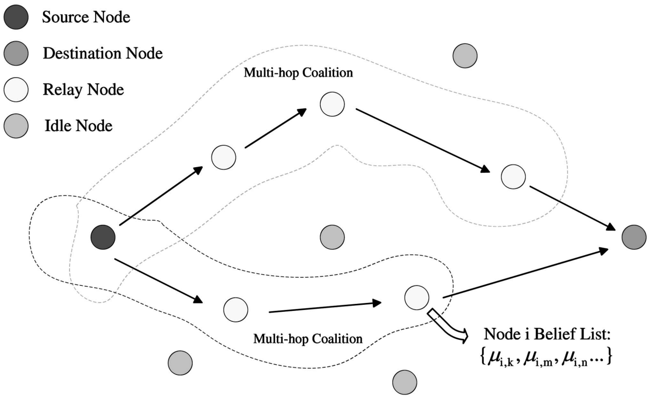


Fig. 3. Belief-based multihop multinode packet forwarding in autonomous MANETs.

sequential equilibrium, we apply it to multihop multinode packet forwarding. In order to cope with more complicated multihop route forming and selection, multiple phases of the strategy are considered. It is worth mentioning that the belief system plays an important role for all strategy phases. Let R_i^t denote the set of players on the forwarding route of player i in tth period. Let $\mu_{i,j}$ denote the sender i's belief value of the node j on the route. The proposed forwarding strategy for the multiplayer case is illustrated as follows:

Belief-based multihop packet forwarding (BMPF) strategy. In the multinode multihop packet forwarding game, given the discount factor δ_G and $p = (p_e, p_f)$, the sender and relay nodes act as follows during different phases of routing process:

- Game partition and belief initialization: Partition the original game into N subgames according to (17). Then, each node initializes its belief of other nodes as $\pi(\delta_G^N, p)$ and forwards packets with probability $\pi(\delta_G^N, p)$.
- Route participation: The selected relay node on each route participates in the routing if and only if its beliefs of the sender and other forwarding nodes are greater than π.
- Route selection: The sender selects the route with the largest $\mu_i = \Pi_{j \in R_i} \mu_{ij}$ with $\mu_{ij} > \pi$ from the route candidates.
- Packet forwarding: The sender updates its belief of each relay node's continuation strategy using (10)-(13) and decides the following actions based on its belief.

The above BMPF strategy in multihop multinode scenario is illustrated in Fig. 3, which shows the multihop coalitions formed by multiple nodes. Note that the idle nodes are the nodes with low belief values observed from other nodes so that they cannot participate on a routing candidate. Fig. 3 also illustrates that each node maintains a list of belief values of all the nodes that it have interactions with.

In the above strategy, the belief value of each node plays an important role. The nodes who intentionally drop packets will be gradually isolated by other nodes since the nodes who have low belief value of the misbehaved nodes will not cooperate with them or participate in the possible routes involving these nodes. During the route participation stage, only the nodes with mutual beliefs that are greater than the cooperation threshold can form a forwarding multihop route. Considering the belief value is defined as the probability of forwarding, it can be directly used for the source node to choose the optimal forwarding route from the routing candidates. It is worth addressing that although the source node is the beneficiary of gains of one transmission stage, the relaying nodes gain the belief from others during this transmission, which will be beneficial to themselves in the future game stages when they need others to forward packets for them. Since the repeated game modeling is applied to model packet forwarding in this paper, the total payoff of each node (source node or relay node) can be improved if it participates in multihop packet forwarding following the BMPF strategy. Note that the equivalent two-player gain g here is different from that in Table 1, which needs to further cope with the error propagation and routing diversity depending on the routing statistics, such as $q_r(r)$ and $q_\hbar(\hbar)$. The roles of sender or relay nodes may change over time depending on which source-destination pair has packets to transmit. As each node is selfish and trying to maximize its own payoff, all nodes are inclined to follow the above strategy for achieving the optimal payoff. In order to formally show the optimality of the proposed BMPF strategy, we have the following theorem:

Theorem 4. *The packet forwarding strategy and belief evaluation system specified by the BMPF Strategy lead to a sequential equilibrium for the multiplayer packet forwarding game.*

Proof. A sequential equilibrium for the game with imperfect information is not only sequential rational but also consistent [17]. First, we prove the sequential rationality of the proposed strategy using the one-step deviation property [17], which indicates that (σ, μ) is sequentially rational if and only if no player i has a history h_i at which a change in $\sigma_i(h_i)$ increases his expected payoff.

In route participation stage, we assume each forwarding node $j \in R_i$ has built up a belief value of the sender i as μ_{ji} and the belief values of any other relay node $k \in R_i$. One-step deviation property is considered for the following three subcases for any forwarding node j: First, if $\mu_{ji} > \pi$ and $\mu_{jk} > \pi, k \neq j$, a one-step deviation is not to participate in the routing. In this case, the forwarding node will miss the opportunity of cooperating with the sender, which has been shown to be profitable for the forwarding node in (8). Second, if $\mu_{ji} < \pi$ and $\mu_{jk} > \pi, k \neq j$, a one-step deviation is to participate in the routing. Since the relay node j will drop the packet from the sender i, the equivalent cooperation gain g in Table 1 will decrease due to packet-drop of the participated nodes, which also decreases the future gain of node j. Although node j does not afford the cost to forward packets for node i, its future gain will be damaged due to a smaller g. Thus, one-step deviation is not profitable in this subcase. Third, if $\mu_{ji} < \pi$ and there exists node k such that $\mu_{jk} < \pi$, the noncooperation forwarding behavior may happen since node j's belief of node k is lower than the threshold π. Such possible noncooperation outcome may decrease the expected equivalent gain g, which results in future payoff loss as (15) shows. Therefore, in all of the above three subcases of

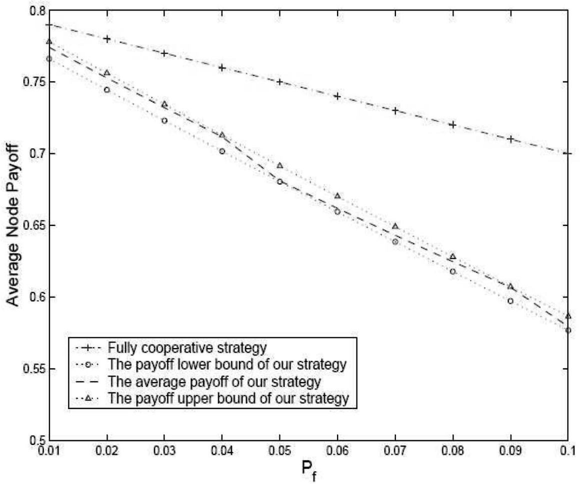


Fig. 4. The average payoffs of the cooperative strategy and proposed strategy.

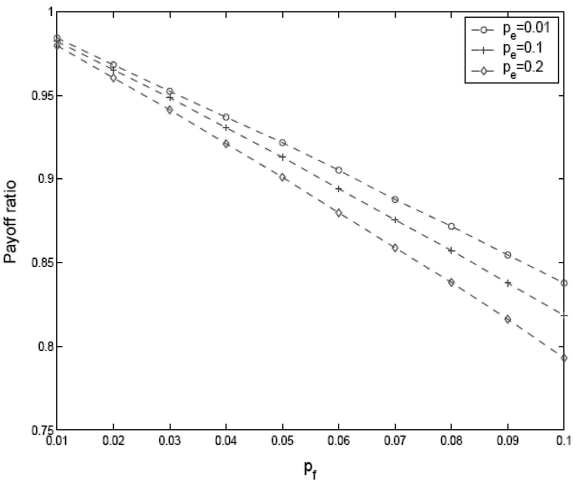


Fig. 5. Payoff ratios of the proposed strategy to the cooperative strategy.

the route participation stage, one-step deviation from the BMPF Strategy cannot increase the payoffs of the nodes.

In route selection stage, two subcases need to be considered for one-step deviation test. First, if the largest μ_i with $\mu_{ij} < \pi, \exists j$ is selected as the forwarding route, there are noncooperation interactions between the sender i and relay j, which decreases the expected equivalent gain g and then lower the future payoffs. Second, if not the route with largest μ_i is selected, the expected gain g can still be increased by another route with larger successful forwarding probability. Thus, one-step deviation is not profitable in the route selection stage.

Further, Theorem 1 can be directly applied here to prove the sequential rationality for every packet forwarding stage. To sum up, the BMPF Strategy is sequential rational for the multinode multihop packet forwarding game. Besides, following the definition of the consistency for sequential equilibria [17], it is straightforward to prove it for our BMPF Strategy. Therefore, the proposed multiplayer packet forwarding strategy is a sequential equilibrium. □

Since the above theorem has proved that the BMPF Strategy is a sequential equilibrium, the cooperation among the nodes can be enforced and no selfish node will deviate from the equilibrium. As all nodes will follow the proposed strategy to have optimal payoffs, the expected gain g in Table 1 can be written as follows:

$$g = \tilde{g} \cdot E_{r,\hbar}[1 - [1 - (\pi(1 - p_f))^{\hbar}]^r] - E(\hbar) \cdot \pi\ell, \qquad (20)$$

where $E(\hbar)$ is the expected number of hops and $E_{r,\hbar}$ represents the expectation with respect to the random variables r and $\hbar$. The first term on the RHS of (20) is the expected gain of the sender considering multiple hops and possible routes; the second term on the RHS is the expected forwarding cost of sender i for returning the forwarding favor of the other relay nodes on its route. Note that π in (20) is also affected by g as shown in (18), which makes the computation of g more complicated. However, as we shown in Theorem 3, the optimal π approaches ϕ when δ approaches $\underline{\delta}$. Considering the situations when δ_G approaches 1, π can be very close to ϕ as $\underline{\delta}$ is approached. Then, we can approximate g by substituting π with ϕ in (20), which is only determined by p_f and p_e.

In addition, in this section, we mainly focus our study on how to build an efficient and formalized belief system that can enforce cooperation in both single-hop and multihop ad hoc networks. Our approach can be applied together with well-studied trust evaluation and propagation models proposed in [13], [15], [16] to propagate and share our defined belief metrics to further enhance the cooperation level in MANETs.

5 Simulation

In this section, we investigate the cooperation enforcement results of our proposed belief evaluation framework by simulation.

We first focus our simulation studies on one-hop packet forwarding scenarios in ad hoc networks, where the two-player belief-based packet forwarding approach can be directly applied to. Let $M = 100$, $g = 1$, and $\ell = 0.2$ in our simulation. In each time slot, any one of the nodes is picked with equal probability as the relay node for the sender. For comparison, we define the cooperative strategy, in which we assume every node will unconditionally forward packets with no regard to other nodes' past behaviors. Such cooperative strategy is not implementable in autonomous ad hoc networks. But it can serve as a loose performance upper bound of the proposed strategy to measure the performance loss due to noisy and imperfect observation.

Fig. 4 shows the average payoff and performance bounds of the proposed strategy based on our belief evaluation framework for different p_f by comparing them with the cooperative payoff. Note that $p_e = 0.01$ and $\delta_G = 0.99$. It can be seen from Fig. 4 that our proposed approach can enforce cooperation with only small performance loss compared to the unconditionally cooperative payoff. Further, this figure shows that the average payoff of our proposed strategy satisfies the theoretical payoff bounds developed in Theorem 3. The fluctuation of the payoff curve of our strategy is because only integer number of subgames can be partitioned into from the original game. Fig. 5 shows the ratio of the

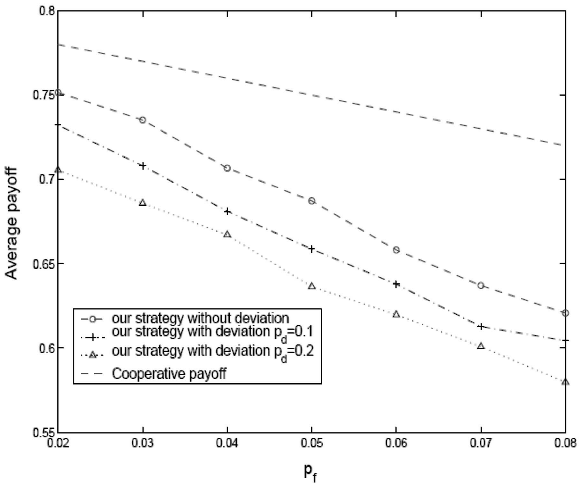


Fig. 6. Payoff comparison of the proposed strategy and deviating strategies.

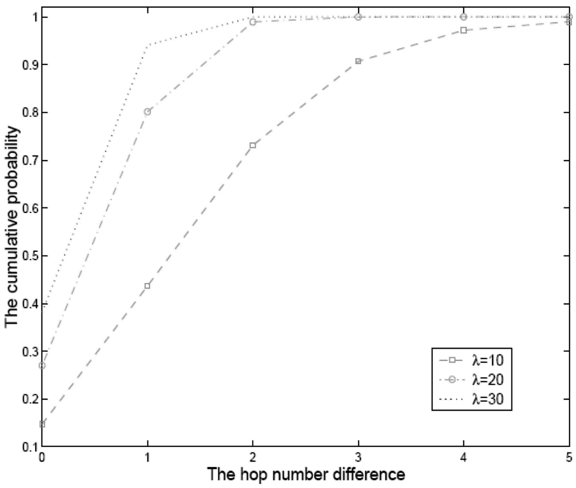


Fig. 7. The cumulative probability mass function of the hop-number difference between the $\tilde{\hbar}(n_i, n_j)$ and $h_{\min}(n_i, n_j)$.

payoffs of our strategy to those of the cooperative strategy for different p_e and p_f . Here, we let $\delta_G = 0.999$ to approach the payoff upper bound. It can be seen from Fig. 5 that even if p_f is as large as 0.1 due to link breakage or transmission errors, our cooperation enforcement strategy can still achieve as high as 80 percent of the cooperative payoff.

In order to show that the proposed strategy is cheat-proof among selfish users, we define the deviation strategies for comparison. The deviation strategies differ from the proposed strategy only when the continuation strategy σ_F and observation F are reached. The deviation strategies will play σ_D with some deviating probability p_d instead of playing σ_F as the proposed belief evaluation framework. Fig. 6 compares the nodes' average payoffs of the proposed strategy, cooperative strategy, and deviation strategies with different deviating probabilities. Note that $\delta_G = 0.999$ and $p_e = 0.1$. This figure shows that the proposed strategy has much better payoffs than the deviating strategies.

Then, we study the performance of the proposed multihop multinode packet forwarding approach. Before evaluating the performance of our proposed strategy, we first need to obtain the routing statistics, such as $q_r(r)$ and $q_{\hbar}(\hbar)$. An autonomous ad hoc network is simulated with $\mathcal{M}$ nodes randomly deployed inside a rectangular region of $10\gamma \times 10\gamma$ according to the 2-dimensional uniform distribution. The maximal transmission range is $\gamma = 100$ m for each node, and each node moves according to the random waypoint model [27]. Let the "thinking time" of the model be the time duration of each routing stage. Dynamic Source Routing (DSR) [27] is used as the underlying routing to discover possible routes. Let $\lambda = \mathcal{M}\pi/100$ denote the normalized node density, i.e., the average number of neighbors for each node in the network. Note that each source-destination pair is formed by randomly picking two nodes in the network. Moreover, multiple routes with different number of hops may exist for each source-destination pair. Since the routes with the minimum number of hops achieve the lowest costs, without loss of generality, we only consider the minimum-hop routes as the routing candidates.

In order to study the routing statistics, we first conduct simulations to study the hop number on the minimum-hop route for source-destination pairs. Let $h_{\min}(n_i, n_j) = \lceil \mathrm{dist}(n_i, n_j)/\gamma \rceil$ denote the ideal minimum number of hops needed to traverse from node i to node j, where $\mathrm{dist}(n_i, n_j)$ denotes the physical distance between node i and j, and let $\tilde{\hbar}(n_i, n_j)$ denote the number of hops on the actual minimum-hop route between the two nodes. Note that we simulate 10^6 samples of topologies to study the dynamics of the routing in ad hoc networks. First, Fig. 7 shows the approximated cumulative probability mass function (CMF) of the difference between the $\tilde{\hbar}(n_i, n_j)$ and $h_{\min}(n_i, n_j)$ for different node densities. Based on these results, the average number of hops associated to the minimum-hop route from node i to j can be approximated using the $\mathrm{dist}(n_i, n_j)$, γ, and the corresponding CMF of hop difference, which also gives the statistics of $q_{\hbar}(\hbar)$. Besides, it can be seen from Fig. 7 that lower node density results in having a larger number of hops for the minimum-hop routes, since the neighbor nodes are limited for packet forwarding in such scenarios. Second, we study the path diversity of the ad hoc networks by finding the maximum number of minimum-hop routes for the source-destination pair. Note that there may exist the scenarios where the node may be on multiple minimum-hop forwarding routes for the same source-destination pair. For simplicity, we assume during the route discovery phase, the destination randomly picks one of such routes as the routing candidate and feeds back the routing information of all node-disjoint minimum-hop routes to the source. Fig. 8 shows the CMF of the number of the minimum-hop routes for different hop number when the node density is 30. This figure actually shows the $q_r(r)$ statistics when the ideal minimum-hop number is given. Based on the routing statistics given in Figs. 7 and 8, we are able to obtain the expected equivalent two-player payoff table for multinode and multihop packet forwarding scenarios using (20).

We compare the payoff of our approach with that of the cooperative one in Fig. 9. Note that multihop forwarding will incur more costs to the nodes since one successful packet delivery involves the packet forwarding efforts of many relay nodes. Also, the noisy and imperfect observation will have more impact on the performance as each

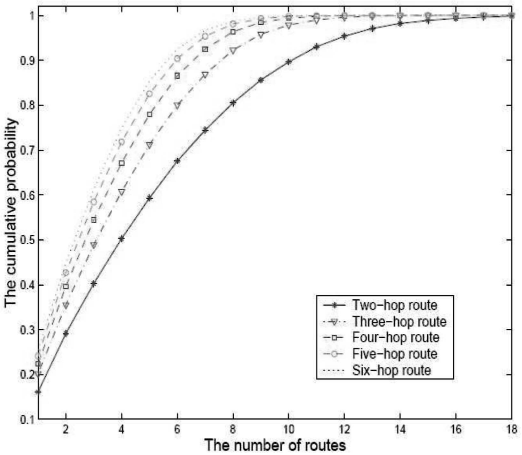


Fig. 8. The cumulative probability mass function of the number the minimum-hop route when the node density is 30.

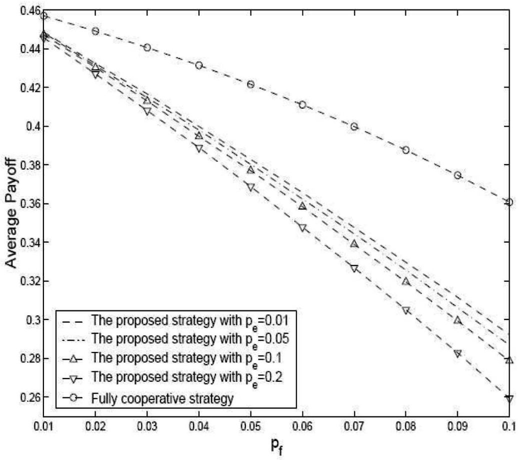


Fig. 9. Average payoffs of the proposed strategy in multinode multihop scenarios.

node's incorrect observation will affect the payoffs of all other nodes on the selected route. We can see from Fig. 9 that our proposed strategy maintains high payoffs even when the environment is noisy and the observation error is large. For instance, when $p_e = 0.2$ and $p_f = 0.1$, our proposed strategy still achieves over 70 percent payoffs of the unconditionally cooperative payoff.

6 Conclusion

In this paper, we exploited how to enforce cooperation in autonomous ad hoc networks under noisy and imperfect observation. The vulnerability analysis is carried out to understand the challenges of achieving cooperation enforcement in the scenarios with noisy and local/imperfect observation. In our approach, by modeling the packet forwarding as a repeated game with imperfect information, we develop the belief evaluation framework for packet forwarding to enforce cooperation in the scenarios with noisy and imperfect observation. It is shown in this paper that the behaviorial strategy with well-defined belief system in our proposed approach can not only achieve the sequential equilibrium for the repeated games, but also have high payoffs. We develop and analyze the belief-based strategy for both the two-node scenario and multinode multihop networking scenarios with only each node's action history and imperfect private observation required for the proposed strategy. The simulation results illustrate that the proposed belief evaluation framework achieves stable and near-optimal equilibria in ad hoc networks under noisy and imperfect observation.

Appendix

Proof of Theorem 1. First, we prove the sequential rationality of the solution obtained by our algorithm. It is already shown in [17] that (σ, μ) is sequentially rational if and only if no player i has a history at which a change in $\sigma_i(h_i)$ increases his expected payoff. This is also called the one-step deviation property for sequential equilibrium, which we use in our proof to show the sequential rational property of the proposed solution. □

There are three possible outcomes considering the relation between μ and π.

1. If $\mu_i(h_i^{t-1}) > \pi$, a one-step deviation from σ^* is to drop packets in current period and continue with σ^* in the next period. Since the action player i chooses is D, the operators (12) and (13) need to be considered for updating beliefs. Noting that $\mu_i(h_i^{t-1}, (D, f))$ is an increasing function with respect to $\mu(h_i^{t-1})$ and $\mu(h_i^{t-1}) \leq 1$, we can obtain that $\mu_i(h_i^{t-1}, (D, f)) < p_e$. Since $\pi > 1/2$ and $p_e < 1/2$, we have the continuation belief satisfying $\mu_i(h_i^{t-1}, (D, f)) < \pi$. Then, only the following two subcases need to be considered:

   a. Suppose $\mu_i(h_i^{t-1}, (D, d)) \leq \pi$. In this case, since $\mu_i(h_i^{t-1}, (D, d)) \leq \pi$ and $\mu_i(h_i^{t-1}, (D, f)) \leq \pi$, the one-step deviation results in the continuation strategy σ_D. Considering the node's current action D, the deviated node will play σ_D in this subcase. But, (8) shows that the rational node prefers σ_F than σ_D when $\mu_i(h_i^{t-1}) > \pi$. Then, a one-step deviation here cannot increase the payoff of the node.
   b. Suppose $\mu_i(h_i^{t-1}, (D, d)) > \pi$. The one-step deviation is to drop packets in current period and continue with σ_D if the history information set (D, f) is reached or continue with σ_F if (D, d) is reached. Compared with the first subcase, we find that the one-step deviation differs from σ_D only when the information set (D, d) is reached. Let $\triangle\hat{V}(\mu)$ be the payoff difference between the proposed solution and the one-step deviation, which can be written as

$$\begin{aligned}\triangle\hat{V}_i(\mu_i^{t-1}) = \triangle V_i(\mu_i^{t-1}) - \delta[\mu_i^{t-1} \cdot p_f \\ + (1 - p_e) \cdot (1 - \mu_i^{t-1})] \cdot \triangle V_i(\mu(h_i^{t-1}, (D, d))),\end{aligned} \tag{21}$$

   where the first term on the RHS is the payoff difference between σ_F and σ_D, and the second term on the RHS is the conditional payoff difference when (D, d) is reached. Noting that (13) indicates $\mu_i(h_i^{t-1}, (D, d)) < \mu_i(h_i^{t-1})$ and

$\triangle V(\mu)$ is an increasing function in μ. we have $\triangle V_i(\mu_i(h_i^{t-1})) > \triangle V_i(\mu_i(h_i^{t-1},(D,d)))$. Moreover, as the coefficient of the second term in (21) is less than one, $\triangle\hat{V}_i(\mu_i(h_i^{t-1}))$ is strictly greater than zero. Thus, the one-step deviation is not profitable in this subcase.

Since there is no subcases other than the above ones, we show that if $\mu_i(h_i^{t-1}) > \pi$, the one-step deviation cannot increase the payoff for the node.

2. If $\mu_i(h_i^{t-1}) < \pi$, a one-step deviation from σ^* is to forward packets in current period and continue with σ^* in the next period. Considering $\pi < \phi$ and $\mu_i(h_i^{t-1},(F,d))$ is an increasing function in $\mu_i(h_i^{t-1})$, we can show that $\mu_i(h_i^{t-1},(F,d)) < 1/2$ if $\mu_i(h_i^{t-1}) < \pi$, thus $\mu_i(h_i^{t-1},(F,d)) < \pi$. Then, there are two subcases:

   a. If $\mu_i(h_i^{t-1},(F,f)) \geq \pi$, the one-step deviation from σ^* becomes playing the cooperation strategy σ_F. As we have shown in (8), σ_D is preferable to σ_F if $\mu_i(h_i^{t-1}) < \pi$.

   b. If $\mu_i(h_i^{t-1},(F,f)) < \pi$, the deviated strategy differs from σ_F only when the private history (F,f) is reached. Let $\triangle\tilde{V}(\mu_i(h_i^{t-1}))$ be the payoff difference between the equilibrium strategy σ_D and the one-step deviation strategy, which can be obtained as

$$\begin{aligned}\triangle\tilde{V}(\mu_i(h_i^{t-1})) &= \triangle V(\mu_i(h_i^{t-1})) - \delta[\mu_i(h_i^{t-1})(1-p_f)\\ &\quad + p_e\cdot(1-\mu_i(h_i^{t-1}))]\cdot\triangle V(\mu_i(h_i^{t-1}),(F,f)).\end{aligned} \tag{22}$$

   Note that $\triangle V(\mu_i(h_i^{t-1})) < \triangle V(\mu_i(h_i^{t-1}),(F,f))$ considering $\mu_i(h_i^{t-1},(F,f)) > \mu_i(h_i^{t-1})$. As the coefficient of the second term on the RHS in (22) is less than one, we have a positive $\triangle\tilde{V}(\mu_i(h_i^{t-1}))$, which shows that the one-step deviation in this subcase cannot increase payoff.

3. If $\mu_i(h_i^{t-1}) = \pi$ the node is indifferent between forwarding packets and dropping packets from (8). Obviously, a one-step deviation will not change the expected payoff.

By studying the above three cases, we prove that the proposed strategy (σ^*,π) of the packet forwarding game is sequential rational when $\pi \in (1/2,\phi)$.

Then, we prove the consistency of the proposed strategy. Since the proposed strategy is a pure strategy when $\mu_i \neq \pi$ we construct a completely mixed strategy $(\sigma_i^\epsilon,\mu_i^\epsilon)$, which is constructed by allowing a tremble with a small probability ϵ from purely forwarding strategy or dropping strategy. By applying (10)-(13) to calculate the belief-update system with tremble, it is easy to show that μ_i^ϵ converges to μ_i when ϵ approaches zero. Therefore, given a sequence $\bar{\epsilon} = (\epsilon_n)_{n=1}^\infty$ satisfying $\lim_{n\to\infty}\epsilon_n = 0$, we can show that the sequence $(\sigma_i^{\epsilon_n},\mu_i^{\epsilon_n})_{n=1}^\infty$ of strategies with completely mixed strategies converges to the proposed strategy (σ^*,μ) while the belief system being updated by Bayes' rule.

Therefore, since the proposed strategy satisfies the sequential rationality and consistency properties when $\pi \in (1/2,\phi)$, it is a sequential equilibrium for the packet forwarding game with imperfect private observation.

Acknowledgments

This paper has been presented in part at the *IEEE Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Virginia, September 2006.

References

[1] C. Perkins, *Ad Hoc Networking.* Addison-Wesley, 2000.

[2] C.K. Toh, *Ad Hoc Mobile Wireless Networks: Protocols and Systems.* Prentice Hall PTR, 2001.

[3] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks" *Proc. ACM MobiCom,* pp. 255-265, Aug. 2000.

[4] P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," *Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security,* 2002.

[5] S. Buchegger and J.-Y.L. Boudec, "Performance Analysis of the CONFIDANT Protocol," *Proc. ACM MobiHoc,* pp. 226-236, 2002.

[6] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," *Proc. IEEE INFOCOM,* 2003.

[7] W. Yu and K.J.R. Liu, "Attack-Resistant Cooperation Stimulation in Autonomous Ad Hoc Networks," *IEEE J. Selected Areas in Comm.,* special issue in autonomic comm. systems, vol. 23, no. 12, pp. 2260-2271, Dec. 2005.

[8] Z. Ji, W. Yu, and K.J.R. Liu, "An Optimal Dynamic Pricing Framework for Autonomous Mobile Ad Hoc Networks," *Proc. IEEE INFOCOM,* 2006.

[9] V. Srinivasan, P. Nuggehalli, C.F. Chiasserini, and R.R. Rao, "Cooperation in Wireless Ad Hoc Networks," *Proc. IEEE INFOCOM,* 2003.

[10] Z. Ji, W. Yu, and K.J.R. Liu, "Cooperation Enforcement in Autonomous MANETs under Noise and Imperfect Observation," *Proc. Third Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON '06),* 2006.

[11] P. Michiardi and R. Molva, "A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks," *Proc. IEEE/ACM Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOPT '03)* 2003.

[12] E. Altman, A.A. Kherani, P. Michiardi, and R. Molva, "Non-Cooperative Forwarding in Ad-Hoc Networks," *Proc. 15th IEEE Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC '04),* 2004.

[13] S. Ganeriwal and M.B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," *Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '04),* Oct. 2004.

[14] F. Li and J. Wu, "Mobility Reduces Uncertainty in MANETs," *Proc. IEEE INFOCOM,* May 2007.

[15] Y. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Information Theoretic Framework of Trust Modeling and Evaluation for Ad Hoc Networks," *IEEE J. Selected Areas in Comm.,* special issue on security in wireless ad hoc networks, vol. 24, no. 2, pp. 305-317, Feb. 2006.

[16] Y. Sun, Z. Han, W. Yu, and K.J.R. Liu, "A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks," *Proc. IEEE INFOCOM,* 2006.

[17] M.J. Osborne and A. Rubinstein, *A Course in Game Theory.* MIT Press, 1994.

[18] D. Fudenberg and J. Tirole, *Game Theory.* MIT Press, 1991.

[19] D. Abreu, P. Milgrom, and D. Pearce, "Toward a Theory of Discounted Repeated Games with Imperfect Monitoring," *Econometrica,* vol. 58, pp. 1041-1063, 1990.

[20] T. Sekiguchi, "Efficiency in Repeated Prisoner's Dilemma with Private Monitoring," *J. Economic Theory,* vol. 76, pp. 345-361, 1997.

[21] V. Bhaskar and I. Obara, "Belief-Based Equilibria in the Repeated Prisoners' Dilemma with Private Monitoring," *J. Economic Theory,* vol. 102, pp. 40-69, 2002.

[22] R.M. Axelrod, *The Evolution of Cooperation.* Basic Books 1984.

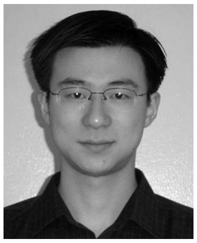
[23] J.J. Jaramillo and R. Srikant, "DARWIN: Distributed and Adaptive Reputation Mechanism for Wireless Ad Hoc Networks," *Proc. ACM MobiCom,* 2007.

[24] D. Bertsekas, *Dynamic Programming and Optimal Control,* second ed., vols. 1 and 2. Athena Scientific, 2001.

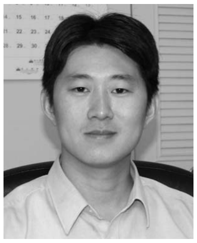
[25] G. Ellison, "Cooperation in the Prisoner's Dilemma with Anonymous Random Matching," *Rev. of Economic Studies,* vol. 61, pp. 567-588, 1994.

[26] L.A. DaSilva and V. Srivastava, "Node Participation in Peer-to-Peer and Ad Hoc Networks: A Game Theoretic Formulation," *Proc. Games and Emergent Behavior in Distributed Computation Workshop,* Sept. 2004.

[27] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing,* pp. 153-181, Kluwer Academic, 2000.



Zhu Ji received the BS and MS degrees in electronic engineering from Tsinghua University, Beijing, China, in 2000 and 2003, respectively, and the PhD degree in electrical and computer engineering from the University of Maryland, College Park in May 2007. He is currently with Qualcomm, San Diego, California. From 2003 to 2007, he was a graduate research assistant in the Communication and Signal Processing Laboratory, University of Maryland, College Park. From 2000 to 2002, he was a visiting student (research intern) in the Wireless and Networking Group at Microsoft Research Asia, Beijing, China. His research interests are in wireless communications and networking.



Wei Yu received the BS degree in computer science from the University of Science and Technology of China (USTC), Hefei, in 2000, the MS degree in computer science from Washington University, St. Louis, Missouri, in 2002, and the PhD degree in electrical engineering from the University of Maryland, College Park, in 2006. From 2000 to 2002, he was a graduate research assistant at Washington University. From 2002 to 2006, he was a graduate research assistant with the Communications and Signal Processing Laboratory and the Institute for Systems Research, University of Maryland. He joined Microsoft Corporation, Redmond, Washington, in 2006. His research interests include network security, wireless communications and networking, game theory, wireless multimedia, handwriting recognition, and pattern recognition.

K.J. Ray Liu is a distinguished scholar-teacher of the University of Maryland, College Park. He is associate chair of Graduate Studies and Research of Electrical and Computer Engineering Department and leads the Maryland Signals and Information Group conducting research encompassing broad aspects of information science and technology including wireless communications and networking, information forensics and security, multimedia signal processing, and biomedical engineering. He is the recipient of numerous honors and awards, including best paper awards from the IEEE and EURASIP, the title of IEEE Signal Processing Society Distinguished Lecturer, the EURASIP Meritorious Service Award, and the US National Science Foundation Young Investigator Award. He also received various teaching and research recognitions from the University of Maryland, including the university-level Invention of the Year Award, and the Poole and Kent Senior Faculty Teaching Award and Outstanding Faculty Research Award, both from A. James Clark School of Engineering. He is a fellow of the IEEE and the AAAS. He is president-elect and was vice president—publications of the IEEE Signal Processing Society. He was the editor-in-chief of the *IEEE Signal Processing* magazine and the founding editor-in-chief of the *EURASIP Journal on Applied Signal Processing*. His recent books include *Cognitive Radio Networking and Security: A Game Theoretical View* (Cambridge University, 2010), *Cooperative Communications and Networking* (Cambridge University, 2008), *Resource Allocation for Wireless Networks: Basics, Techniques, and Applications* (Cambridge University, 2008), *Ultra-Wideband Communication Systems: The Multiband OFDM Approach* (IEEE-Wiley, 2007), *Network-Aware Security for Group Communications* (Springer, 2007), *Multimedia Fingerprinting Forensics for Traitor Tracing* (Hindawi, 2005), and *Handbook on Array Processing and Sensor Networks* (IEEE-Wiley, 2009).