Ad Hoc Networks 8 (2010) 181–192

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

A protocol for data availability in Mobile Ad-Hoc Networks in the presence of insider attacks

E. Ayday *, F. Fekri

School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA

ARTICLE INFO

Article history:
Received 31 December 2008
Received in revised form 9 June 2009
Accepted 10 July 2009
Available online 17 July 2009

Keywords:
Trust
Reputation
Security
Game theory

ABSTRACT

In Mobile Ad-Hoc Networks (MANETs), establishing trust relationships between the nodes in a decentralized fashion has been an important research issue for a long time. If the sender nodes accurately identify the legitimate nodes in the network, a robust routing can be provided while mitigating the effects of malicious nodes. Further, there is always a mutual interaction between a sender and its neighbor nodes during the communication. This mutual interaction can be easily modeled as a game between two or more players (one player being the sender and the rest being the receivers). Regardless of its type (legitimate or malicious), each player attempts to maximize its benefit during the game by choosing an optimal strategy. In this paper, we propose a secure and robust routing scheme in which the interaction between the sender and receiver nodes is modeled using a dynamic Bayesian game model. A repeated game is considered and opinions of a node about the types of other nodes is established using an acknowledgement mechanism from the destination. The proposed method uses the intersection of game theory, trust establishment and coding theory to resist colluding Byzantine (insider) attacks. The scheme guarantees the availability of message as long as a legitimate path exists. Through simulations we will show the efficiency of the scheme with respect to latency, availability and energy consumption in the presence of adversary.

Published by Elsevier B.V.

1. Introduction

Mobile Ad-Hoc Networks (MANETs) play key roles in many military and civilian applications such as battlefields, environment monitoring and emergency response. The lack of infrastructure in MANETs requires the network nodes to implement the network tasks by themselves. Hence, network operation is based on the cooperation of nodes within neighborhood. For routing, intermediate nodes are used to forward a packet from a source to a destination node. Therefore, security becomes a challenging problem in this multihop environment with unreliable intermediate nodes.

The main threat for routing in a MANET is the existence of selfish and malicious nodes. The goal of a selfish node is to maximize its own welfare, on the other hand a malicious node tries to prevent the network from operating efficiently or properly. Without any countermeasures against these threats, the network performance decreases considerably.

We propose a secure and efficient routing scheme using a game theoretical approach and trust relationships between the nodes. We assume a "Dynamic Bayesian Game" model [1] among the nodes to find the optimal strategies of legitimate and malicious nodes. Moreover, using the "watchdog" technique [2] and the "acknowledgement" mechanism (ACK), we construct trust relationships between the nodes. Recent works [2–10] either do not consider the malicious nodes or build the trust relationships based on the watchdog mechanism, which has serious

* Corresponding author. Tel.: +1 404 518 7037; fax: +1 404 894 8363.
E-mail addresses: erman@ece.gatech.edu (E. Ayday), fekri@ece.gatech.edu (F. Fekri).

1570-8705/$ - see front matter Published by Elsevier B.V.
doi:10.1016/j.adhoc.2009.07.001

drawbacks in a wireless medium (especially in the presence of malicious nodes). Our main objective in this work is to mitigate the effects of malicious nodes to the network performance by establishing trust relationships and using a game theoretical approach between the network nodes. The network under interest is a MANET. Moreover, the network is assumed to be connected at any time instant. In other words, we assume that a path can be established between any two nodes at any time.

The rest of this paper is organized as follows. In the rest of this section, we summarize the related work in trust establishment and game theory in ad hoc networks and also mention the contributions of this paper. A brief description of the scheme is provided in Section 2. In Section 3, we analyze the game model, describe the parameter selection and show how the game changes dynamically. Trust establishment and using the trust values (node credentials) are studied in Section 4. In Section 5, we describe the adversarial model and the possible threats specific to our scheme. We evaluate and compare our scheme using computer simulations in Section 6. Eventually, the concluding remarks are provided in Section 7.

1.1. Related work

The main goal for building trust values (node credentials) among the nodes in MANETs is to protect Dynamic Source Routing (DSR) [11] from attackers and increase the performance of the network. In MANETs, a node evaluates another by using either direct or indirect measurements. Direct measurements are the ones that the node conducts itself to rate another node. On the other hand, indirect measurements are the ones that are received from other nodes regarding the credential of a specific node. Building node credentials by direct measurement is either achieved by using the watchdog mechanism or by using the ACK from destination. Building node credentials by relying on the direct measurements and using the watchdog mechanism is proposed in [2,3,5]. The purpose of the watchdog mechanism is to identify a malicious node by overhearing the communication of the next hop. In [2,3], when a misbehavior is detected, it is reported to the source of the communication and the source updates the credential for the detected node. In [5], legitimate nodes reject the traffic initiated by the detected malicious nodes. In [6,7,4,12–14], the use of indirect measurements to build node credentials is also allowed while the watchdog mechanism is used to obtain the direct measurements. In [12,13], credentials obtained by direct and indirect measurements are updated using the Bayesian approach. [14] proposes an information theoretical approach to trust and reputation. Some major drawbacks of using the watchdog mechanism to obtain direct measurements are listed below:

1. The fact that the monitoring node (the one which uses the watchdog mechanism) hears the transmission of its next hop does not mean that the following node in the path actually receives the packet. In other words, a malicious node may transfer a packet such that its previous-hop neighbor (who uses the watchdog mechanism) hears the transmission while its next-hop neighbor (who is supposed to receive the packet) does not. This can easily be achieved by adjusting the transmission power of the antenna (given that the previous-hop neighbor is located closer than the next-hop neighbor) or by using a directional antenna. Hence, the malicious node achieves its goal by preventing the legitimate flow without being penalized.
2. When there are consecutive malicious nodes in the path, it becomes very easy to cheat a monitoring node and gain credit for a malicious node (even though it keeps misbehaving). If one of the next-hop neighbors of a malicious node is also malicious, it can always send its packets to its malicious neighbor. Hence, its previous-hop neighbor (who uses the watchdog mechanism) hears the legitimate transmission and gives credit to the malicious node while its malicious next-hop neighbor drops the packets to prevent the legitimate flow.

We note that it is not guaranteed that the scenarios we listed above will occur all the time. However, as the malicious nodes in the network and the resources of the adversary increases, it is very likely to observe these scenarios. Hence, we claim that relying on the watchdog mechanism to obtain direct measurements (hence, to build trust relationships) is deceptive and misleading most of the time.

In [15,16], node credentials are constructed using the ACK messages sent by the destination node. The major drawback of these schemes is that, if a path dies due to a malicious node, the source will need to retransmit all the packets it sent via a different path. Moreover, the diversity of latency for different paths can affect the overall scheme negatively. On the other hand, as we will describe, our scheme does not suffer from this because of the use of rateless coding. In [15,16], possible routes from the source to the destination are established before the data transfer begins. Hence, even if one node is compromised from these routes, data availability is lost even though source and destination may have other alternative paths. In contrast, our scheme provides data availability as long as there is a legitimate path between the source and destination, since we construct the paths on-the-fly using our trust-metric.

Recently, researches started to use game theory to analyze wireless networks. Especially Bayesian game theoretical model [1] is commonly used to analyze wireless networks with selfish/attacker nodes. In reputation based schemes which use the Tit-for-tat strategy (e.g., [6,17]), each node monitors its neighbors and behaves based on the previous behavior of its neighbors. However, in these schemes, even if all the nodes are willing to cooperate, packet collision or noise may infer with accurate monitoring, resulting in zero throughput even if there is no malicious node in the network. Generous Tit-for-tat is proposed in [8] to fix this problem. However, to achieve full cooperation in [8], the probability that a forwarded packet was not overheard by the originating node (p_e) should be accurately estimated. In [9], authors proposed a reputation mechanism called DARWIN which does not depend on the perfect estimation of p_e. However, the scheme does not consider malicious nodes and assumes that all nodes share their perceived dropping probabilities

with each other. A Bayesian attacker/defender game is studied in [10]. Optimal behaviors of the defender and attacker is analyzed for static and dynamic Bayesian games. However, the game is only between two players and the trust values (credentials) of the players are calculated only by using the watchdog mechanism. On the other hand, we consider a game between a legitimate sender and the combination of legitimate and malicious receivers. Further, we do not use the watchdog mechanism to update the opinions of the nodes for their neighbors.

1.2. Contributions of our scheme

The main contributions of our scheme are summarized in the following.

1. By the intersection of the trust establishment, the game theoretic approach and modern error control coding, we provide a robust scheme with low latency and high data availability in the presence of the adversary.
2. As opposed to previously proposed trust management schemes (which use game theory), we consider a game between more than two network nodes, and find the optimal behaviors of all the nodes which are involved in the game.
3. We provide a robust scheme against the collaboration of malicious nodes. Most of the previous schemes which only depend on the watchdog mechanism (to build the trust relationships) are vulnerable to the collaboration of malicious nodes. On the other hand, our scheme guarantees the delivery of the message packets as long as a legitimate path exists between the source and the destination. This robustness comes with communication/computation efficiency.
4. In the proposed scheme the paths from the source to the destination are established on-the-fly by the back pressure policy. Hence, the latency and data availability of our scheme do not suffer when a specific path involves malicious or selfish nodes. Moreover, this mechanism encourages to use the paths that provide the lowest latency even if there is no malicious activity in the network.

2. Description of the scheme

2.1. Overview of the scheme

The proposed scheme mainly consists of three mechanisms; game between the nodes, trust establishment and rateless coding. In general, the game theory studies the interactions between the players. In a typical game, a player tries to maximize its benefit by choosing the correct strategy considering the strategies of the other players. When the cost and gain of a player depends on the strategies of the other players, game theory helps to find the optimal strategies of all players. This model is perfectly analogous with the interaction between the legitimate and malicious nodes in wireless networks. In a typical network, the main goal of the legitimate nodes is to make sure that all the network operations are proceeding properly. On the other hand, the goal of the malicious nodes is to prevent the network operations as much as possible. Hence, legitimate nodes try to detect and isolate the malicious nodes and malicious nodes try to give the most harm to the network while staying undercover (not detected) to achieve their goals and maximize their outcome. Thus, we decided to analyze the mutual action between the nodes using a game theoretical approach. In our model, the players are the nodes in the network, and the game is between a legitimate sender and its next hop neighbors (potential receivers). The main goal of the sender (a source or an intermediate node) is to forward the packets it received (or generated) to the destination reliably and as soon as possible. Hence, it expects its next hop neighbors to have the same goal. As opposed to a legitimate node, the main goal of a malicious node is to decrease the performance of the network by increasing the total latency, decreasing data availability or increasing the energy consumption of the legitimate nodes. Hence, a malicious node often tends to drop the legitimate packets or to forward modified packets so as to prevent the sender from achieving its goal. However, a malicious node has to take part in the ongoing communication (i.e., be part of the path) to give damage. On the other hand, a legitimate sender is always inclined to select its next hop neighbors (potential receivers) among those which would help to achieve its goal. Hence, there is a game between the legitimate sender and its potential receivers to achieve their goals in which each node has to select an optimal strategy to maximize its benefit.

A legitimate sender node always tends to select its most trustworthy neighbors as its potential receivers. In order to find out the most trustworthy neighbors, a trust establishment mechanism is required. Most previous schemes such as [4,5] use the watchdog mechanism to build the trust values (credentials) of the nodes. However, due to some serious shortcomings of this mechanism (discussed in Section 1.1), we use the ACK message from the destination to build the node credentials. Based on the ACK messages, a legitimate sender node selects its potential receivers (among its next hop neighbors) which help maximizing its benefits for the rest of the communication session. We note that the type of trusted nodes may change or a legitimate node may fail between two consecutive ACK messages. Hence, in addition to choosing the most trustworthy neighbors (as its potential receivers), a legitimate sender needs to determine its packet forwarding strategy among those chosen neighbors based on their behaviors up until it receives the next ACK message. For this purpose, a legitimate node uses the watchdog mechanism to monitor its neighbors and to take countermeasures against the malicious ones. It is worth noting that we do not use the watchdog mechanism to build the node credentials. It is used as a tool to enhance the scheme when the drawbacks mentioned in Section 1.1 does not occur (when there are no consecutive malicious nodes on the path or when the malicious node has limited resources). Even when the watchdog mechanism is cheated by the malicious nodes, node credentials are calculated accurately as the watchdog mechanism has no effect on the calculation of the node credentials. In other

words, the drawbacks of the watchdog mechanism do not have any impact on the node credentials in the proposed scheme.

In our model, the source node encodes its packets before sending them to the destination using rateless codes [18,19]. The rational for this is to avoid retransmissions, decrease total latency and increase availability at the destination. If the original message packets are used without encoding, whenever the destination does not receive a subset of the original packets, the sender has to resend those missing packets until they are received. However, using the rateless codes, the source keeps generating and sending new packets until the destination receives sufficient number of packets to decode for the original message.

2.2. Description

In order to facilitate future references, frequently used notations are listed in Table 1 with their meanings.

We assume the source node has t number of packets $(w_1, w_2, \ldots, w_t)$ to send. Using rateless coding [18,19], these packets are encoded into T packets $Q_1, Q_2 \ldots$ as illustrated in Fig. 1a. The encoding process can be summarized as follows:

1. Pick a generator polynomial $\Omega(x) = \sum_{1 \leqslant i \leqslant t} \Omega_i x^i$ where $\Omega_i \in [0, 1]$ for $i = 1, \ldots, t$ and $\Omega(1) = 1$.
2. Generate and instance, say z, of a random variable Z with distribution Ω.
3. Pick z distinct packets at random from the input t data packets.
4. XOR the selected packets and declare as the encoded packet.

It is proved in [18] that, t original packets can be recovered from any $T = t + O(\sqrt{t}\ln^2(t/\delta))$ of the encoded packets with probability $1 - \delta$. Hence, rateless coding decreases the total latency and increases availability (even in the presence of adversary) by helping the destination to get the original message from any subset of the received legitimate packets. When the destination receives sufficient number of packets, it decodes the received packets to obtain the original data as illustrated in Fig. 1b. We summarize the decoding process as follows:

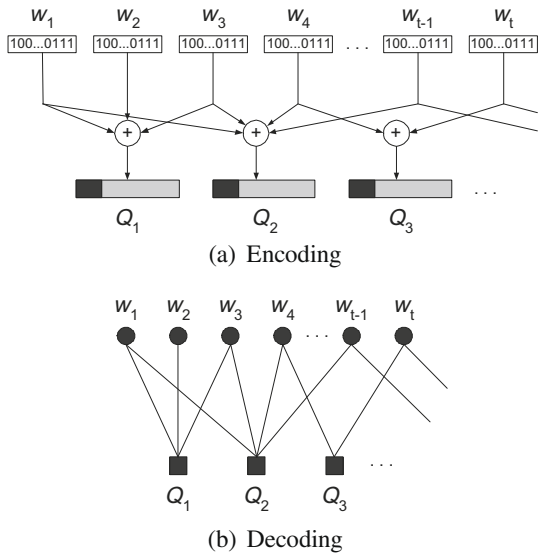


Fig. 1. Illustration of encoding and decoding of rateless codes.

1. Wait until T packets are received.
2. Construct the Tanner graph between the encoded and the data packets.
3. Use Message Passing Decoding [23,24] to recover data packets.

After generating the encoded packets, if confidentiality is required, the source node may encrypt each encoded packet Q_i using the pairwise key shared between itself and the destination node. By doing so, the source node prevents the eavesdroppers and intermediate nodes from revealing the content of the original message.

Even though the adversary cannot reach the content of the original message, it may try to prevent the destination from getting the message by modifying the packets or injecting noise to them (the complete adversary model and the possible threats due to the adversarial nodes are described in Section 5). To prevent this type of attacks, authentication tags are attached to each encoded packet at the source. Hence, when a malicious node modifies a packet, it is detected immediately at the next hop (if the

Table 1
Notations.

N	Total number of nodes in the network
T	Number of encoded packets that should be received by the destination for complete message recovery
$slot_T$	Duration of a time-slot
ACK_T	Acknowledgement period (from the destination)
P_b^a	Probability of node a being malicious in the eyes of node b
$P_{w_a}^i$	Probability that node i uses its watchdog mechanism for its neighbor node a
P_{att}^i	Attacking probability for a malicious node i
max_n	Maximum number of neighbors (potential receivers) a sender node may use within a time-slot
W_s^i	The event, node s uses its watchdog mechanism for node i
$\overline{W_s^i}$	The event, node s does not use its watchdog mechanism for node i
A_i	The event, malicious node a misbehaves
$\overline{A_i}$	The event, malicious node a does not misbehave

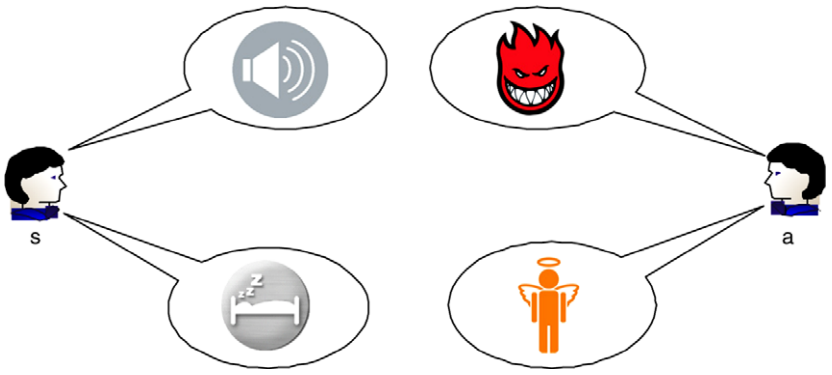


Fig. 2. Illustration of the game between the sender s and the malicious receiver a.

next hop is a legitimate node, otherwise the first legitimate node who receives the packet will detect). Thus, the malicious packet will not be forwarded to the destination and the resources of the legitimate nodes will not be consumed. Moreover, if the previous hop of the malicious node is in watchdog phase, it can also detect the misbehavior and take the necessary countermeasures against it as explained in Section 4. We note that message confidentiality and packet authentication are not the main goals of this work. Hence, we mention these issues only for the sake of completeness.

Packets are sent from the source to the destination in a hop-by-hop fashion. During the packet forwarding, each node (legitimate or malicious) chooses its next move to maximize its benefit in the game. As illustrated in Fig. 2, a legitimate sender node (s) just forwards its packets and chooses whether to use its watchdog mechanism or to stay passive depending on the trust value (credential) of its receiver. A malicious receiver node (a), on the other hand, decides whether to attack or not depending on the watchdog strategy of its previous hop. As we mentioned before, we do not use the watchdog mechanism to built the node credentials. Hence, node credentials are not affected by the possible flaws in the watchdog mechanism (which were discussed in Section 1.1. We describe the game model in detail in the next section.

We divide the time into time-slots of length $slot_T$. At the beginning of a time-slot, each sender node finds out its potential receivers (among its one-hop neighbors) based on a metric which depends on the credentials of its neighbors and their distances to the destination. We assume that during a time-slot, the neighbors of a node remain the same. Legitimate nodes use the ACK from the destination to build the trust values (credentials) of their neighbors and determine their optimal behaviors. ACKs are sent by the destination node with a specific period which is ACK_T. We observed via simulations (in Section 6) that the choice of ACK_T does not have a significant effect on the total latency and data availability. We note that ACK is sent for the block of packets that the destination has received between two ACK periods and the length of the ACK packet is negligible with respect to the data packets. Building the trust values are explained in detail in Section 4.

3. Game model

3.1. Analysis of the game

We consider the interaction between a legitimate sender node and its receivers. The legitimate node picks its max_n neighbors as its potential receivers based on a metric depending on neighbors' credentials and distances to the destination (as explained in Section 4). In our model, each legitimate node only knows the probabilities of its neighbors being malicious. The sender has two possibilities after sending the packet. It may decide to use its watchdog mechanism to see whether its next hop neighbor is misbehaving, or it may decide not to use it (so it will not consume extra energy). For simplicity of discussion, we illustrate the game for the sender s and the receivers a and b (when $max_n = 2$). In order to calculate the payoffs of the sender and the receivers, we introduce the costs of possible incidents in Table 2.

Based on the previous observations of the sender s (ACKs received from the destination), the probabilities of node a and node b being malicious are P_s^a and P_s^b, respectively. Further, a node being malicious does not imply that it will behave maliciously all the time. Hence, given a and b are malicious, we define the attacking probabilities for nodes a and b as P_{att}^a and P_{att}^b, respectively.

Table 2
Costs of possible incidents.

C_f	Cost of forwarding a packet
C_r	Cost of receiving a packet
C_{WD}	Cost of using watchdog mechanism per packet
C_A	Cost of attacking per packet
G_{ch}	Gain of a malicious node when it succeeds to cheat a legitimate node
L_{ch}	Loss for a legitimate node when it is cheated ($G_{ch} = L_{ch}$)
G_{ca}	Gain for a legitimate node when it succeeds to detect a misbehavior
L_{ca}	Loss for a malicious node when its misbehavior is detected ($G_{ca} = L_{ca}$)
G_{pr}	Gain for a potential receiver when another receiver is detected while it is misbehaving

Given the sender s communicates with node a, the total payoff of s when it uses its watchdog mechanism can be obtained as

$$G_s(W_s^a) = P_{att}^a P_s^a[-C_f - C_{WD} + G_{ca}] + (1 - P_{att}^a) \times P_s^a[-C_f - C_{WD}] + (1 - P_s^a)[-C_f - C_{WD}]. \quad (1)$$

Similarly, when the communication is between s and node b, the payoff of s becomes

$$G_s\left(W_s^b\right) = P_{att}^b P_s^b[-C_f - C_{WD} + G_{ca}] + \left(1 - P_{att}^b\right) \times P_s^b[-C_f - C_{WD}] + (1 - P_s^b)[-C_f - C_{WD}]. \quad (2)$$

On the other hand, when s chooses not to use its watchdog mechanism, its total payoffs when communicating with nodes a and b becomes

$$G_s(\overline{W}_s^a) = P_{att}^a P_s^a[-C_f - G_{ch}] + (1 - P_{att}^a) P_s^a[-C_f] + (1 - P_s^a)[-C_f] \quad (3)$$

and

$$G_s(\overline{W}_s^b) = P_{att}^b P_s^b[-C_f - G_{ch}] + \left(1 - P_{att}^b\right) P_s^b[-C_f] + (1 - P_s^b)[-C_f], \quad (4)$$

respectively. However, s uses both nodes a and b as its potential receivers during a time-slot. Hence, combine (1) with (2) and (3) with (4) to get the total payoff of the sender s. We define f_a (forwarding probability for node a) and f_b (forwarding probability for node b) as the probabilities that s will choose node a and b to forward a packet, respectively (computing these probabilities will be explained in Section 4). Therefore, the total payoffs of s for using and not using its watchdog mechanism becomes

$$\begin{aligned} G_s(W_s) = {} & f_a\{P_{att}^a P_s^a[-C_f - C_{WD} + G_{ca}] + (1 - P_{att}^a) P_s^a[-C_f - C_{WD}] \\ & + (1 - P_s^a)[-C_f - C_{WD}]\} + f_b\left\{P_{att}^b P_s^b[-C_f - C_{WD} + G_{ca}]\right. \\ & \left. + \left(1 - P_{att}^b\right) P_s^b[-C_f - C_{WD}] + \left(1 - P_s^b\right)[-C_f - C_{WD}]\right\} \end{aligned} \quad (5)$$

and

$$\begin{aligned} G_s(\overline{W}_s) = {} & f_a\{P_{att}^a P_s^a[-C_f - G_{ch}] + (1 - P_{att}^a) P_s^a[-C_f] \\ & + (1 - P_s^a)[-C_f]\} + f_b\left\{P_{att}^b P_s^b[-C_f - G_{ch}]\right. \\ & \left. + \left(1 - P_{att}^b\right) P_s^b[-C_f] + \left(1 - P_s^b\right)[-C_f]\right\}, \end{aligned} \quad (6)$$

respectively. Using (5) and (6), we conclude that, if $G_s(W_s) > G_s(\overline{W}_s)$, the sender s will choose to use its watchdog mechanism, because it gains more versus not using it. However, if the sender always uses the watchdog mechanism, the rational strategy for the malicious receiver node will be not to misbehave at all (as it will be detected and punished each time it misbehaves). On the other hand, if $G_s(W_s) < G_s(\overline{W}_s)$, then s will choose not to use the watchdog mechanism. However, in this case the malicious receiver node will choose to attack as it will not be detected by s. As a result, we propose to equate the payoffs $G_s(W_s)$ and $G_s(\overline{W}_s)$ to use a mixed strategy. Hence, by using a mixed strategy, we obtain the following:

$$f_a P_{att}^a P_s^a + f_b P_{att}^b P_s^b = \frac{C_{WD}}{G_{ch} + G_{ca}}. \quad (7)$$

This illustrates the optimal attacking probabilities for nodes a and b (if they are malicious). This result can be easily generalized to $max_n > 2$. For $max_n = I$, the combined attacking probabilities of next hop neighbors of node s can be obtained as

$$f_1 P_{att}^1 P_s^1 + f_2 P_{att}^2 P_s^2 + \ldots + f_I P_{att}^I P_s^I = \frac{C_{WD}}{G_{ch} + G_{ca}}. \quad (8)$$

It is also required to analyze the communication from the receiver's side to determine the optimal watchdog strategy of the sender s. For this analysis, it is sufficient to focus on one receiver and calculate the payoffs of that receiver for different behaviors. First, we will assume that node a is malicious and calculate its payoffs when it misbehaves and behaves as a legitimate node, respectively. We let $P_{w_a}^s$ be the watchdog probability of node s for node a. Then, the payoff of node a for attacking becomes

$$\begin{aligned} G_a(A_a) = {} & f_a\{P_{wa}^s[C_f - C_r - C_a - G_{ca}] \\ & + (1 - P_{wa}^s)[C_f - C_r - C_a + G_{ch}]\} + f_b\left\{P_s^b P_{att}^b P_{wb}^s\right\} G_{pr}. \end{aligned} \quad (9)$$

In (9), the last term $f_b\{P_s^b P_{att}^b P_{w_b}^s\}G_{pr}$ represents the profit gained by node a if node b is detected and punished by the sender s when it is misbehaving (this mechanism will be explained in more detail in Section 4). Similar to (9), the payoff of node a when it chooses not to attack can be represented as

$$\begin{aligned} G_a(\overline{A}_a) = {} & f_a\{P_{wa}^s[C_f - C_r] + (1 - P_w a^s)[C_f - C_r]\} \\ & + f_b\left\{P_s^b P_{att}^b P_{wb}^s\right\} G_{pr}. \end{aligned} \quad (10)$$

If $G_a(A_a) > G_a(\overline{A}_a)$, then the malicious node will always prefer to attack. However, in this case, the sender s will decide to use its watchdog mechanism constantly. On the other hand, if $G_a(A_a) < G_a(\overline{A}_a)$, then the attacker's strategy will be not to attack. Therefore, node s will never need to use its watchdog mechanism and there will not be any problems in the network (attacker will not give any harm to the network). As a result, we propose to use a mixed strategy as we did before by equating the payoffs (9) and (10). By doing so, we obtain the following watchdog probability for the sender (representing how often the sender s should use its watchdog mechanism for the receiver node a).

$$\widehat{P}_{w_a}^s = \frac{-C_a + G_{ch}}{G_{ch} + G_{ca}}. \quad (11)$$

The probability in (11) is calculated with the assumption that the node a is malicious. Thus, we need to multiply (11) with the probability of node a being malicious in the eyes of sender s. Hence, we illustrate the optimal watchdog probability of the sender in the following:

$$P_{w_a}^s = P_s^a \frac{-C_a + G_{ch}}{G_{ch} + G_{ca}}. \quad (12)$$

In the next section, we will describe how to compute the parameters in (7) and (12).

3.2. Parameter selection for the game

In this section, we will itemize the key issues for parameter selection.

1. In (12), to satisfy the axioms of probability, we require $G_{ch} \geqslant C_a$ and $(G_{ca} + C_a) \geqslant 0$.
2. To make the model simpler, we assume that the cost an attacker pays when it is detected is equal to its gain when it attacks without being detected. Hence, $G_{ca} = G_{ch}$.
3. The legitimate node's gain via detecting a malicious node should be greater its loss for monitoring. Otherwise, a legitimate node will never prefer to use its watchdog mechanism. Thus, $G_{ca} > C_{WD}$.
4. We assume that there is no node in the network that is 100% trustworthy. Hence, we define a minimum value for P_s^i as P_s^{min}. Further, we define a minimum value for f_i as f_{min}. The rational is that if f_i approaches to zero the corresponding node would have a negligible forwarding probability. Hence, when the forwarding probability for a node decreases below f_{min}, the sender node decides not to use that node as a receiver until its f_i value increases above that limit again.
5. The optimal attacking probability for the malicious nodes is derived in (8). To satisfy the axioms of probability, the following should be satisfied.

$$\frac{C_{WD}}{G_{ch} + G_{ca}} \leqslant min\{f_i P_s^i\}, i = 1, \ldots, I, \tag{13}$$

where $max_n = I$ and $min\{f_i P_s^i\}$ can be easily calculated for different max_n values.

3.3. Dynamic game

In this section, we will briefly show the dynamic changes during the game and the responses of the players against those changes. First, we will observe the impact when the malicious nodes increase their attacking probabilities from the optimal one which is derived in (8). We assume $max_n = 2$, sender s has potential receivers a and b (among its one-hop neighbors), and at least one of the neighbors is malicious. The combined optimal attacking probability for the neighbor nodes is given in (7). If a malicious node decides to increase its attacking probability, then the left hand side of (7) will also increase. Hence, the difference between the total payoffs of the sender s for the events W_s and $\overline{W}_s$ becomes

$$G_s(W_s) - G_s(\overline{W}_s) = (G_{ch} + G_{ca}) + \left(f_a P_{att}^a P_s^a + f_b P_{att}^b P_s^b\right) - C_{WD}. \tag{14}$$

When the attacking probability of a malicious node increases, the difference in (14) becomes positive (the difference is zero in optimal case). In other words, using watchdog mechanism will become more beneficial to the sender s, which causes the sender node s to increase its watchdog probability $P_{w_a}^s$ or $P_{w_b}^s$.

The increase in the watchdog probability of the sender node also effects the total payoffs of attacker nodes. Assuming nodes a and b are malicious and legitimate, respectively, the difference between the payoffs of node a for the events A_a and $\overline{A}_a$ is illustrated in the following:

$$G_a(A_a) - G_a(\overline{A}_a) = f_a[-P_{w_a}^s(G_{ch} + G_{ca}) - C_a + G_{ch}] \tag{15}$$

From (15), we can say that when the sender s increases its watchdog probability $P_{w_a}^s$, the result of (15) becomes negative (it was zero in the optimal case). In other words, the malicious node a gains more when it chooses not to attack. Hence, node a will decide to reduce its attacking probability P_{att}^a. As we illustrated here with this simple example, increasing the attacking probability to above the optimal value provides no extra gain for a malicious node. Moreover, the malicious node will prefer to decrease its attacking probability further when it realizes that it would gain more with a lower attacking probability.

It is worth noting that the dynamic Bayesian game described throughout this section has a *Perfect Bayesian Equilibrium* (PBE) that is proved in [10].

4. Trust establishment

4.1. Building credentials

Node Credentials take values between zero (i.e., malicious) and one (i.e., trustworthy). Credentials are built by using the ACK from the destination node. Destination node sends ACK packets to its downstream region with a period of ACK_T. A node which receives this ACK packet identifies the IDs of the packets that are received by the destination thus far. When the ACK is received from the destination at time t, a legitimate node first determines the packet with the maximum ID (max_{ID}) that is received by the destination. Then, the credential for the neighbor node i(CR_i) is updated based on the Beta distribution $\left(CR_i = \frac{\alpha+\alpha_t}{\alpha+\alpha_t+\beta+\beta_t}\right)$ as in [20]. Here, β_t stands for the number of packets sent to node i by the sender that has IDs smaller than or equal to max_{ID}, and α_t stands for the number of packets that are included in the ACK message among those β_t packets. Moreover, α and β represent the previous history of node i in the eyes of the legitimate sender. We note that the initial values for the α and β values are 1. Hence all nodes start with a credential of 0.5, which means each node may be a malicious node with a probability of 0.5 initially.

The ACK period (i.e., the time elapsed between two ACKs), ACK_T, is smaller than a time-slot duration, $slot_T$. As ACK_T decreases, intermediate nodes and the source will be able to update the credentials more often. However, sending ACK packets with a high frequency may result in congestions and increase in the energy consumption. Hence, the ACK_T is a network parameter that should be adjusted to maximize the efficiency and security together. We note that because of the multihop communication, some paths may deliver the packets slower than the others. Hence, the nodes in the slower path will also get low credentials even though they might be legitimate. This may seem as if we give low credentials to the legitimate nodes. However, by doing so, we differentiate between the good (fast) and bad (slow) paths even if there is no malicious node participated in those paths.

4.2. Neighbor selection

At the beginning of each time-slot, each node selects its max_n neighbors to use as its potential receivers during that time-slot. This neighbor selection is based on the credentials of the neighbor nodes and their distances to the destination. A sender node i calculates the metric for one of its one-hop neighbors j as in the following:

$$M_j^i = \frac{min[dist]}{dist(j)} \times \frac{cred(j)}{max[cred]}, \tag{16}$$

where $dist(j)$ and $cred(j)$ are the nodes j's distance to the destination and its credential at node i. Further, $min[dist]$ is the minimum of the node i's neighbors' distances to the destination and $max[cred]$ is the largest credential among the neighbors of node i. Node i ranks order its neighbors based on their metric values and selects max_n neighbors with the highest metric values as its potential receivers. This neighbor selection process is illustrated in Fig. 3a for $max_n = 2$.

4.3. Forwarding probabilities

A sender node assigns forwarding probabilities to its potential receivers (chosen among its one-hop neighbors) and chooses them based on these probabilities for packet forwarding (illustrated in Fig. 3b for $max_n = 2$). At the beginning of each time-slot, these probabilities are determined based on the credentials of the neighbors. If we consider the same scenario we discussed before (sender s and receivers a and b), sender s initially determines the forwarding probabilities of nodes a and b based on P_s^a and P_s^b, respectively. Hence, initially s assigns $f_a = (1 - P_s^a)/\left[(1 - P_s^a) + (1 - P_s^b)\right]$ and $f_b = (1 - P_s^b)/\left[(1 - P_s^a) + (1 - P_s^b)\right]$.

These forwarding probabilities are subject to change during the time-slot as a result of the watchdog mechanism. When the sender detects a misbehavior about the receiver i, its forwarding probability is decreased by ϵ, and this decrease is rewarded proportionally to other nodes depending on their credentials. Thus, the sender modifies node j's forwarding probability as $f_j + \epsilon\left\{\left(1 - P_s^j\right)/\left[\left(1 - P_s^1\right) + \cdots + \left(1 - P_s^I\right)\right]\right\}$ (for $max_n = I$). We note that the forwarding probabilities for the potential receivers of a sender node are subject to change for each individual packet. Thus, given when $max_n = I$, we illustrate the expected forwarding probability f_i^k for node i and the k^{th} forwarded packet in the following:

$$f_i^k = f_i^{k-1} - \epsilon f_i^{k-1}\left(P_s^i P_{att}^i P_{w_i}^s\right) + \epsilon \frac{1 - P_s^i}{(1 - P_s^1) + \ldots + (1 - P_s^I)} \times \sum_{j \neq i} f_j^{k-1}(P_s^j P_{att}^j P_{w_j}^s). \tag{17}$$

5. Adversary model

We consider the insider adversary who is allowed to do anything that a legitimate network node can do. An insider adversary takes part in the ongoing transmission, drops the legitimate packets that it receives, modifies the legitimate packets before it forwards them to the next hop or tries to reveal the message sent from the source to the destination. We note that these attacks has a serious impact on the latency, throughput and data availability. Moreover, we consider that multiple malicious nodes may collaborate to achieve a common goal.

In this work we assume that a malicious node behaves maliciously (drops or modifies the packets) with some probability. That is to say, a malicious node behaves as a legitimate node occasionally to remain under cover. Specific attacks that can be mounted against the proposed scheme are listed as follows:

- Since a node determines the credentials of its neighbors by itself, a malicious node is free to assign any credential value to its neighbors. Hence, it will choose to give the highest credential to its malicious neighbors.

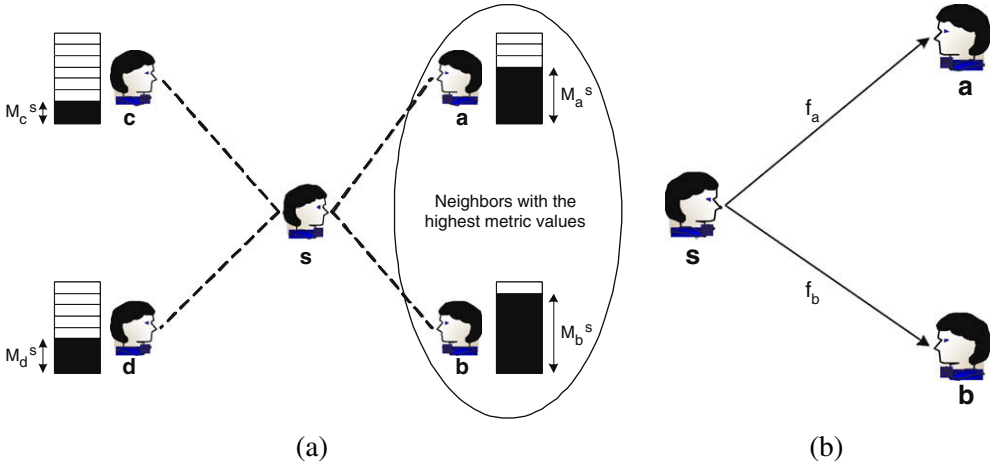


Fig. 3. (a) Neighbor selection process and (b) packet forwarding probabilities.

- At the beginning of each time-slot, each node picks its max_n potential receivers. During this selection phase, a malicious node picks its malicious neighbors regardless of their metric values. Hence, more malicious nodes can be involved in the communication, which will increase the latency.
- In general, a malicious node determines its optimal attacking probability based on (7). However, if the previous neighbor of a malicious node is also malicious, then it does not need to follow the rules of the game, because it knows that it will not be detected. Hence, we assume that consecutive malicious nodes on a path collaborate with each other.

6. Simulations

In order to illustrate the performance of our scheme and see the effects of different design parameters, we evaluate the proposed scheme via computer simulations. The parameters we use for our simulations are listed in Table 3. We assume that nodes move inside a specific boundary based on the "random-way-point" (RWP) model [21]. Hence, we describe the movement pattern of independent nodes by simple terms. At the end of each time-slot, each node moves to its new location based on the RWP model and finds its new neighbors at the new location. For simplicity of routing, we assume that the paths are stable during a time-slot. Moreover, to avoid any packet collusion in the wireless medium, we assume the existence of a medium access control (*MAC*) which controls the nodes who get access to the channel. For this purpose, we use the *MAC* algorithm in [22].

The main purpose of our simulations is to examine the latency, throughput, energy consumption and data availability in the presence of malicious nodes. Throughout our simulations, we assume the existence of insider malicious nodes whose behaviors are explained in Section 5.

We define the probability of data availability as a function of time. If the destination node, on the average, receives sufficient number of packets (to decode the rateless code for the original message) in a definite time t_s, then we say that the scheme provides 100% availability at time t_s. As long as the network is connected, destination will certainly receive enough number of packets if it waits sufficiently long enough. This is because the source is capable of generating unlimited number of packets via rateless coding. However, malicious nodes try to decrease data availability at time t by dropping or modifying the data packets. In our simulations, we measure this decrease in data availability with increasing number of malicious nodes and with different design parameters. Moreover, we measure the change in energy consumption of the network for different adversarial models and design parameters.

We compare our scheme with three different schemes: (1) *defenseless* scheme, in which there is no mechanism against the malicious nodes, (2) *no-ACK* scheme, in which nodes just use the watchdog mechanism to observe and evaluate their next hop neighbors, and (3) *no-WD* scheme, in which nodes do not use the watchdog mechanism and solely use the ACK from the destination to evaluate the other nodes. We note that these three schemes also illus-

Table 3
Simulation parameters.

N	100
T	1000
Communication range	0.45 units
Network area	2 units
RWP range	0.3,0.6 units
Number of trials	100
max_n	2
Number of malicious nodes	$0,\ldots,70$
$slot_T$	100 time units
ACK_T	20,50,100 time units
P_s^{min}	0.1
f_{min}	0.2
ϵ	0.1
G_{ch}	50 units
G_{ca}	50 units
C_a	1 unit
G_{pr}	1 unit
C_{WD}	10 units

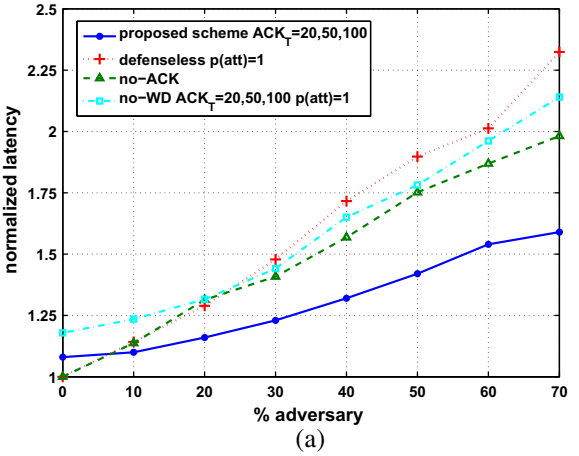
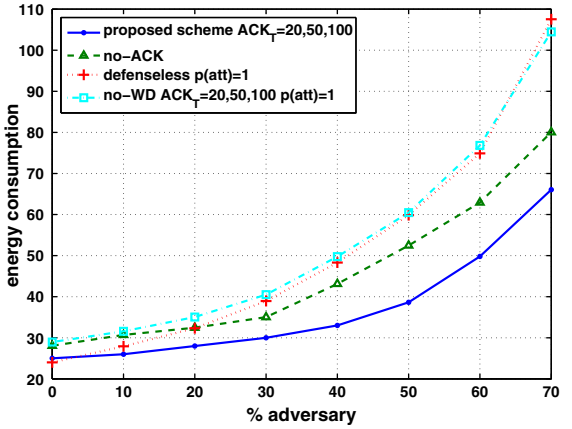


Fig. 4. Comparison of latency and average throughput versus fraction of malicious nodes for four different schemes.

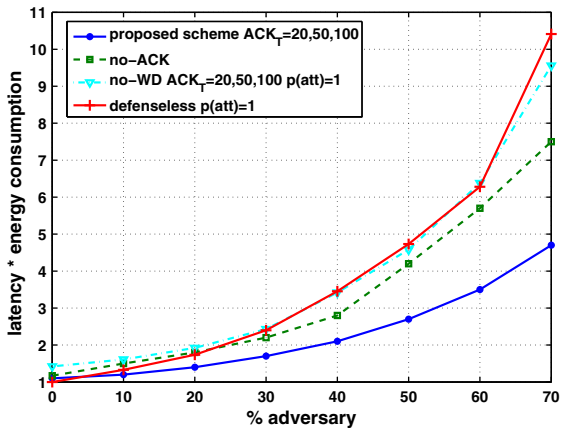
trate the techniques that are used in the recent works which are presented in Section 1.1. Moreover, in all these three schemes, we assume that the source uses the rateless encoding to make a fair comparison with the proposed scheme.

First, we study the effect of malicious nodes to the total latency. We note that there is no game between the nodes in both the *defenseless* and *no-WD* schemes because legitimate nodes do not use the watchdog mechanism. Hence, for these two schemes attacker nodes are free to choose their attacking probabilities independent of the legitimate nodes. We simulated these two schemes for attacking probabilities of 0.2, 0.5 and 1, and observed that the attacker gives the most severe damage when the malicious nodes attack with probability 1. Hence, we use attacking probability, $p(att)$, as 1 when comparing these two schemes with our scheme and the *no-ACK* scheme.

In Fig. 4a, we show the normalized latency versus different number of malicious nodes for different schemes and with different parameters. We normalize the latency value using the latency of the defenseless scheme as a base when there are no malicious nodes in the network. We observe that, the latency of the proposed scheme and *no-WD* scheme are not significantly affected with the change in ACK_T. Hence, we conclude that, as the number of malicious nodes increases, the proposed scheme becomes the most robust one in terms of total latency.

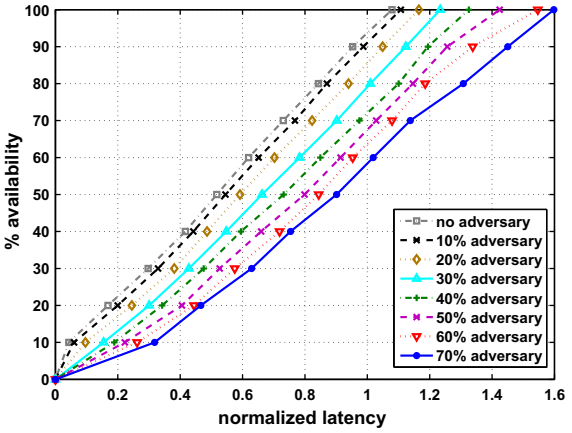


(a)

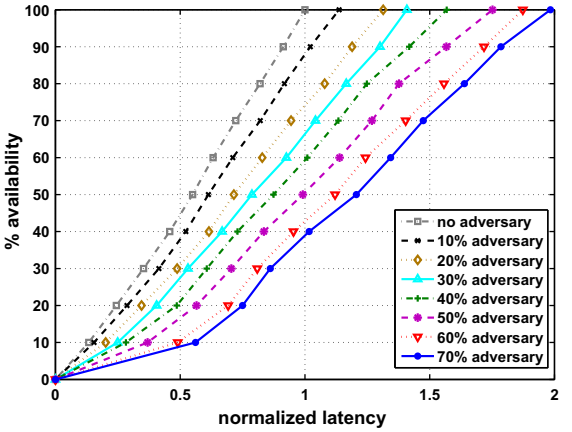


(b)

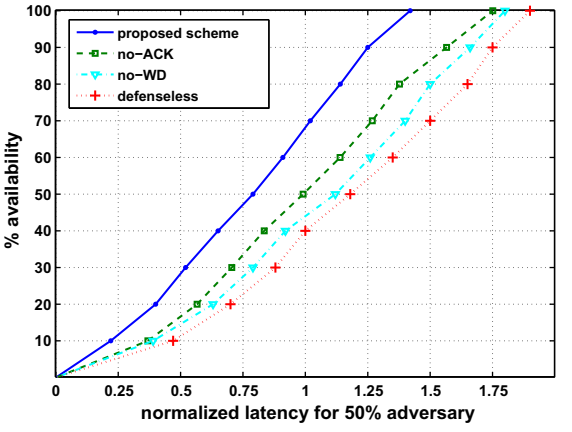
Fig. 5. Energy consumption and *latency* × *energy consumption* versus fraction of malicious nodes.



(a)



(b)



(c)

Fig. 6. Availability versus latency: (a) proposed scheme, (b) *no-ACK* scheme, (c) comparison of all schemes when 50% of nodes are compromised.

We also examine the average throughput of each scheme in Fig. 4b. Here, the vertical axis illustrates the average number of packets received by the destination node in 1000 time units. Similar to the latency simulation, as the number of malicious nodes increases, our scheme provides the highest average throughput.

Next, we consider the energy consumption of each scheme. Since, the average energy consumption is dominated by the energy consumption due to communication, we only consider the number of packet transmissions for a legitimate node. As illustrated in Fig. 5a, the proposed scheme has the lowest energy consumption as it provides high data availability sooner than the other schemes.

We also calculate the normalized *latecy* $\times$ *energy consumption* metric to compare the four schemes. In Fig. 5b, it is shown that *no-ACK* schemes has the closest performance to the proposed scheme. However, as we discussed in Section 1.1, calculating the node credentials based on the watchdog mechanism (as in the *no-ACK* scheme) is not reliable especially when there are two or more consecutive malicious nodes exist on the path.

Finally, we study the data availability versus latency. In Fig. 6a and b the change in availability with the normalized latency is shown for the proposed scheme and the *no-ACK* scheme, respectively. We observe that as the number of malicious nodes increases, our scheme provides higher data availability with lower latency. Furthermore, in Fig. 6c, we show the change in data availability of all schemes when 50% of the nodes are compromised. Hence, we can confidently say that our scheme provides the highest data availability as the number of malicious nodes increases.

We note that as we mention in Table 3, we also simulated each scheme with *RWP range* $= 0.6$ and obtained very close results as we did for *RWP range* $= 0.3$. Hence we do not presented the results for *RWP range* $= 0.6$.

7. Conclusions

This paper was concerned with secure and efficient routing in the presence of malicious nodes, where adversary may compromise nodes, then drops or modifies packets, injects bogus packets or mounts routing attacks. We proposed a routing scheme which depends on the trust establishment and a dynamic Bayesian game model between the network nodes. Besides we used rateless codes at the source to avoid retransmissions and to increase data availability. We showed upon simulations that the proposed scheme provides low latency and high data availability while keeping the energy consumption moderately low even in highly adversarial environments.

References

[1] D. Fudenberg, J. Tirole, Game Theory, The MIT Press, Cambridge, MA, 1991.

[2] S. Marti, T. Giuli, K. Lai, M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in: Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom00), 2000, pp. 255–265.

[3] K. Paul, D. Westhoff, Context aware detection of selfish nodes in dsr based ad-hoc networks, in: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM02), 2002, pp. 178–182.

[4] S. Buchegger, J. Boudec, Performance analysis of confidant protocol (coorperation of nodes: Fairness in dynamic ad-hoc networks), in: Proceedings of the IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, CH, 2002.

[5] S. Bansal, M. Baker, Observation-based cooperation enforcement in ad hoc networks, Research Report cs.NI/0307012, 2003.

[6] Q. He, D. Wu, P. Khlosa, Sori: a secure and objective reputation-based incentive scheme for ad hoc networks, in: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC 2004), Atlanta, GA, 2004, pp. 825–830.

[7] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: Proceedings of IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 2002, pp. 107–121.

[8] F. Milan, J.J. Jaramillo, R. Sirikant, Achieving cooperation in multihop wireless networks of selfish nodes, Workshop on Game Thory for Networks (GameNets 2006), Pisa, Italy, 2006.

[9] J. Jaramillo, R. Srikant, Darwin: distributed and adaptive reputation mechanism for wireless ad-hoc networks, in: Proceedings of ACM International Conference on Mobile Computing and Networking (MobiCom07), Montreal, Quebec, Canada, 2007, pp. 87–98.

[10] J. Liu, C. Comaniciu, H. Man, A bayesian game approach for intrusion detection in wireless ad hoc networks, Workshop on Game Thory for Networks (GameNets 2006), Pisa, Italy, 2006.

[11] D. Johnson, Routing in ad hoc networks of mobile hosts, in: Proceedings of Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, 1994.

[12] S. Buchegger, J. Boudec, A robust reputation system for p2p and mobile ad-hoc networks, in: Proceedings of the Second Workshop on the Economics of Peer-to-Peer Systems, 2004.

[13] S. Ganeriwal, M. Srivastava, Reputation-based framework for high integrity sensor networks, in: Proceedings of the Second ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004, pp. 66–77.

[14] Y. Sun, W. Yu, Z. Han, K. Liu, Information theoretic framework of trust modeling and evaluation for ad hoc networks, the IEEE Journal on Selected Areas in Communications 24 (2) (2006) 305–317.

[15] P. Dewan, P. Dasgupta, A. Bhattacharya, On using reputations in ad hoc networks to counter malicious nodes, in: Proceedings of the Tenth International Conference on Parallel and Distributed Systems (ICPADS04), 2004.

[16] A.S.A. Mahmoud, S. El-Kassas, Reputed authenticated routing for ad hoc networks protocol (reputed-aran), in: Proceedings of the Second ACM International Workshop on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks, 2005, pp. 258–259.

[17] R. Mahajan, M. Rodrig, D. Wetherall, J. Zahorjan, Sustaining cooperation in multihop wireless networks, in: Proceedings of the Second USENIX Symposium on Networked System Design and Implementation (NSDI 05), Boston, MA, 2005.

[18] M. Luby, LT codes, in: Proceedings of the IEEE Symposium on Foundations of Computer Science. Vancouver, 2002, pp. 271–280.

[19] A. Shokrollahi, Raptor codes, IEEE Transactions on Information Theory 52 (6) (2006) 2551–2567. Jun.

[20] S. Buchegger, J. Boudec, The effect of rumor spreading in reputation systems for mobile ad-hoc networks, in: Proceedings of Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt 03), 2003.

[21] C. Bettstetter, H. Hartenstein, X. Perez-Costa, Stochastic properties of the random waypoint mobility model, Wireless Networks 10 (5) (2004) 555567.

[22] W. Ye, J. Heidemann, D. Estrin, An energy-efficient mac protocol for wireless sensor networks, in: Proceedings of the IEEE Conference on Computer Communications (INFOCOM02), 2002.

[23] T.J. Richardson, R.L. Urbanke, The capacity of low-density parity check codes under message-passing decoding, IEEE Transactions on Information Theory 47 (2001) 599–618. Feb..

[24] G.D. Forney, Jr., On iterative decoding and the two-way algorithm, in: Proceedings of International Symposium on Turbo Codes and Related Topics, 1997.

Erman Ayday received his B.Sc. degree in electrical and electronics engineering from Middle East Technical University, Ankara, Turkey, in 2005. He received his M.S. degree in electrical and computer engineering from School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, in 2007. He is currently a Research Assistant in the Information Processing, Communications and Security Research Laboratory and pursuing his Ph.D. degree at the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA. His current research interests include wireless network security, game theory for wireless networks and trust and reputation management.

Faramarz Fekri received the B.Sc. and M.Sc. degrees from Sharif University of Technology, Tehran, Iran, in 1990 and 1993, respectively, and the Ph.D. degree from the Georgia Institute of Technology, Atlanta, in 2000. From 1995 to 1997, he was with the Telecommunication Research Laboratories (TRLabs), Calgary, AB, Canada, where he worked on multicarrier spread spectrum systems. Since 2000, he has been with the faculty of the School of Electrical and Computer Engineering, Georgia Institute of Technology. His current research interests lie in the general field of signal processing and communications, in particular, wavelets and filterbanks, error control coding, cryptography, and communication security. In the past, he conducted research on speech and image processing. Dr. Fekri received the 2000 Sigma Xi Best Ph.D. Thesis Award from the Georgia Institute of Technology for his work on finite-field wavelets and their application to error control coding. He also received the National Science Foundation CAREER award in 2001.