WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
*Wirel. Commun. Mob. Comput.* 2014; **14**:1450–1470
Published online 7 September 2012 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2271

RESEARCH ARTICLE

# Trust establishment in cooperative wireless relaying networks

Reyhaneh Changiz[1]*, Hassan Halabian[1], F. Richard Yu[1], Ioannis Lambadaris[1] and Helen Tang[2]

[1] Department of Systems and Computer Engineering, Carleton University, 1125 Colonel By Drive, Ottawa, ON, K1S 5B6, Canada
[2] Defense R&D Canada, Ottawa, ON, Canada

## ABSTRACT

In cooperative wireless networks, relay nodes are employed to improve the performance of the network in terms of throughput and reliability. However, the presence of malicious relay nodes in the network may severely degrade the performance of the system. When a relay node behaves maliciously, there exists a possibility that such a node refuses to cooperate when it is selected for cooperation or deliberately drops the received packets. Trust establishment is a mechanism to detect misbehaving nodes in a network. In this paper, we propose a trust establishment method for cooperative wireless networks by using Bayesian framework. In contrast with the previous schemes proposed in wireless networks, this approach takes the channel state information and the relay selection decisions into account to derive a pure trust value for each relay node. The proposed method can be applied to any cooperative system with a general relay selection policy whose decisions in each cooperative transmission are independent of the previous ones. Moreover, it does not impose additional communication overhead on the system as it uses the available information in relay selection procedure. Copyright © 2012 John Wiley & Sons, Ltd.

**KEYWORDS**

trust establishment; cooperative relaying; Bayesian methodology

***Correspondence**

Reyhaneh Changiz, Department of Systems and Computer Engineering, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada.
E-mail: rchangiz@sce.carleton.ca

## 1. INTRODUCTION

Cooperative relaying is considered as a promising technique to improve the performance of wireless communication systems in terms of throughput, reliability, and efficiency. In this type of communication, one or more relay nodes are involved to cooperatively transmit the information to the destination. Cooperation of relay nodes with the source node can take place in various layers of communication networks, for example, physical, medium access control, and network layers. In this paper, our focus will be on cooperative communication in the physical layer. It has been shown that cooperation can lead to capacity improvement by providing spatial diversity and higher efficiency because of spatial multiplexing [1–4]. Although much research work has been carried out on cooperative communication, most of which concentrates on efficiency and capacity analysis, and a little considers security problems in these networks. Security is a challenging issue in cooperative communication networks as the source node has to rely on intermediate relay nodes to transmit its information.

Different security mechanisms for wireless networks have been established in literature. Usually, these mechanisms can be classified as *prevention*-based and *detection*-based techniques. This classification of security mechanisms is defined on the basis of their timing approach and the specific area of their targeted application. In the following, a brief description of each type is provided.

- Prevention-based: the goal is to employ some prevention techniques such as encryption/decryption, data origin authentication, and integrity protection. In fact, these types of techniques are the security mechanisms that act at the front line of defence to avoid any attack or unauthorized action by malicious or adversarial nodes and provide integrity, confidentiality, and nonrepudiation of communications [5–7].

- Detection-based: the goal is to ensure that any adversarial or misbehaving node that had entered the network can be traced and separated from the network (e.g., intrusion detection systems) [8–18].

Although cryptographic techniques provide promising approaches to make the system secure, there still remains the chance for compromised relay nodes to take part in the cooperation process and disrupt the transmissions. Another example is the case where a selfish (and not necessarily compromised) relay node refuses to cooperate or deliberately drops the received packets (for different reasons, e.g., power saving) when it is selected for cooperation. Henceforth, we will refer to such misbehaving relay nodes as malicious nodes.

Misbehavior of malicious relay nodes may deteriorate the performance of the system severely. This motivates us to look for a detection-based mechanism that can distinguish the misbehaving relay nodes from the benign ones. To this end, each relay node is associated with a real value from the interval $[0, 1]$, which is called *trust* representing to what extent it is trustworthy for cooperation. In general, trust of an entity is defined as the probability that it performs a specific action expected of it [19]. In cooperative wireless systems, each relay node is expected to forward the received packets to the destination when it is selected for cooperation. Trust establishment is a scheme to evaluate and assign a trust value to each cooperating entity in the network, which enables the trustor (e.g., network controller) to detect the misbehaving nodes.

In this paper, our objective is to design a trust establishment scheme for cooperative relaying networks. We consider a cooperative network consisting of one source node $S$, one destination node $D$, and $R$ relay nodes in between. The source is transmitting its information with the cooperation of one of the relay nodes according to a two-phase cooperation protocol. In the first phase of the cooperation protocol, the source node broadcasts the information to the relay nodes as well as the destination. In the second phase, one of the relay nodes is selected by node $D$ for cooperation according to an employed relay selection policy and transmits the information to the destination. Note that node $D$ not only is the destination of information but also carries out the role of selecting the relay nodes and hence is a network controller. Finally, node $D$ combines the signals received in the the first and the second phases (e.g., by using maximum ratio combining (MRC) [20]) and detects the information from the combined signal. In such a network, the trust of a given relay node will decrease if and only if it misuses the opportunity of cooperative transmission or refuses to cooperate intentionally when it is selected for cooperation. Bayesian trust establishment methodology is known to be a promising trust establishment technique used in wireless ad hoc networks [12,15]. In Section 4.2, we will review Bayesian trust establishment methodology in detail.

Our contributions in this paper can be summarized as follows: by using an example, we first show that the conventional Bayesian trust establishment technique cannot be directly applied in wireless cooperative relaying networks as the obtained trust values will be biased on the relay selection policy and system channel condition. Thus, we propose a trust establishment scheme for wireless cooperative relaying networks based on the Bayesian methodology that takes into account the relay selection decisions and channel condition information in the trust computation. The proposed method can be applied to any system with a general relay selection policy whose decisions in each cooperative transmission are independent of the previous ones. Moreover, our method does not impose additional communication overhead on the system because it uses the available information in the relay selection procedure. Simulations are conducted to show the effectiveness and accuracy of the proposed scheme. We also examine the proposed methodology in a multiuser cooperative system and a cellular relaying system and show its effectiveness in computing pure trust values for all the relay nodes.

The rest of the paper is organized as follows. In Section 2, we will review the related work in this area of research. In Section 3, we provide a detailed description of the cooperative system used in this paper. Two fundamental concepts of trust and Bayesian methodology are reviewed in Section 4. The proposed trust establishment method for cooperative relaying networks is introduced in Section 5. We demonstrate the accuracy of the proposed method by simulation results presented in Section 6. A summary of this work and discussion for future directions are presented in Section 7.

## 2. RELATED WORK

In this section, we briefly review the related research work in the area of detection-based security mechanisms in cooperative wireless networks. We also review the trust establishment schemes especially Bayesian trust establishment technique in wireless ad hoc networks. On the basis of our knowledge, the trust establishment technique proposed in this paper is the first work that considers Bayesian trust establishment in wireless cooperative networks.

Detection-based security techniques in cooperative communication have been considered in a small number of papers. Indeed, most of the research in this area is concentrated on secrecy rate analysis (and not trust computation) in physical layer in the presence of malicious relay nodes [8,9,13,14,21,22]. In [21], the authors considered a source–destination pair that is communicating only through an unauthenticated relay node. The goal is to keep the source information transmission secret from the relay node. The authors proposed a cooperative jamming scheme to assure the security of the communication between the source and the destination. In the proposed jamming scheme, the destination jams the relay and uses the jamming message signal as the side information to detect the source signal. The authors proved that a positive secrecy rate is achievable. Although the proposed jamming scheme guarantees a

positive secrecy rate, it does not provide a detection mechanism to identify the malicious relay nodes. In [14,22], secret communication between the source and the destination nodes with authenticated relay nodes has been considered. The message communicated to the destination is going to be kept information-theoretically secret from any eavesdropper. In [22], the authors proved the existence of a trade-off between the achievable reliable transmission rate and the amount of information leaked to an eavesdropper over an arbitrary wireless relay network. The work in [14] uses a similar setting and introduces three cooperative schemes including decode-and-forward (DF), amplify-and-forward, and cooperative jamming. For all the cases, the optimal cooperation strategy (optimal weighting of the relay node signals) that maximizes the achievable secrecy rate subject to a transmission power constraint was determined. Note that the goal in the analysis of [14,22] was to keep the information secret from the eavesdropper. However, the authors did not propose any specific mechanism to detect the malicious nodes.

The work in [8,9] considered the security issues in the cooperative communications that consist of multiple relay nodes and one adversarial relay node who tries to corrupt the communications by sending garbled signals. The authors proposed a cross layer detection-based technique that traces the adversarial nodes by using adaptive signal detection at the physical layer while employing pseudo-random tracing symbols in the application layer. Note that the proposed scheme in [8,9] is effective for systems with multiple cooperative relay nodes without relay selection. However, for the relaying systems where we have to perform relay selection among all the existing relay nodes, this scheme cannot be applied. Moreover, it does not explicitly provide an applicable detection-based technique for identifying the malicious nodes. A signal detection technique was proposed in [13] to mitigate maliciousness of a malicious relay node by having the destination examine the relay's signal before applying diversity combining with the direct signal from the source. The proposed technique compares the signals received from the two diversity branches to determine the relay's behavior. It is shown that a malicious relay reduces the correlation between the received signals in the diversity branches. In [13], it has been shown that the proposed technique improves the performance of the system in terms of bit error rate (BER) and outage probability. However, it does not contribute to an explicit statistical detection-based security mechanism that identifies the malicious relay nodes from the benign ones. Moreover, the analysis does not incorporate the relay selection process for a system with multiple relays.

As we explained in the previous section, our focus in this paper is to study the trust establishment in cooperative wireless systems. Thus, in the following, we review the existing trust establishment techniques in wireless networks. A large body of research in trust management in wireless networks has focused on trust establishment in mobile ad hoc networks (MANETs) [12,15–18]. In [16], the authors proposed a trust establishment method with high adaptability for MANETs based on game theory. The advantage of the proposed method is that it does not impose heavy communication overhead on the system and the trust computation convergence is fast. However, the proposed scheme does not incorporate the indirect evidences from other nodes in the trust estimation process. Authors in [17] elaborate upon issues related to trust and introduce a context-aware reputation-based method of trust establishment. The proposed method is a decentralized scheme that is independent of the underlying cryptographic schemes and mitigates the chances of having a prejudiced opinion. In [18], a secure authentication approach for multicast MANETs is proposed, employing a Markov chain trust model to determine the trust value for each one-hop neighbor. Note that the proposed schemes in [17,18] were proposed for MANETs, and their application in wireless cooperative networks requires further considerations.

Bayesian methodology is a well-known approach for trust establishment [23,24] in wireless ad hoc networks. It is widely used for computation of trust in wireless networks particularly in [12,15,25]. In Bayesian methodology assuming that every transmission is independent of previous transmissions, trust values are derived as the mean of a Beta distribution function. The parameters of Beta distribution function are obtained by performing iterative observations on the system. After each observation period, the parameters of the Beta function are updated according to a recursive formula on the basis of the previous parameters and the new observation information. In [15], Bayesian methodology was used to compute trust values in MANETs, and a distributed reputation system was constructed accordingly. The objective in [12] is to achieve a trust establishment method to have reliable data packet delivery. The approach is based on Bayesian methodology using trust and confidence values that are computed to construct a reputation model. We will show by an example that the conventional Bayesian techniques proposed in [12,15] cannot be directly applied in wireless cooperative networks because they do not consider the channel condition and relay selection in the trust computation. In [25], the authors designed a trust-assisted cooperative transmission scheme. The trust model they employed is based on Bayesian methodology similar to the work in [12]. In their approach, maliciousness and unreliability of channels are taken into consideration simultaneously for signal combining at the destination. Although the proposed scheme can improve the system throughput, no detection-based security mechanism was provided for detecting malicious relay nodes.

In [10,11], we proposed a trust establishment methodology based on the Bayesian framework. In contrast with the previous schemes, this approach takes the channel state information and relay selection policy into account to derive a pure trust value for each relay node. The proposed method can be applied to any system with a general relay selection policy whose decisions in each cooperative transmission are independent of the previous ones. The results of this paper complement the results of [10,11] by

providing more detailed discussions and explanations and a comprehensive set of simulations. The simulations are evaluating the performance of the proposed trust establishment method with the conventional Bayesian method in single source system (with and without combining), in a multiuser system with multiple sources and multiple relay nodes, and in a cellular system with mobile users and mobile relays.

## 3. SYSTEM DESCRIPTION

In this section, we introduce the cooperative communication system used in this paper. We will describe the topological configuration of the network and the cooperative communication protocol used in our system as well as the communication parameters and settings (e.g., channel, power, noise, and modulation). We also introduce the relay selection policy that we employed in our system. As we discussed earlier, the proposed trust establishment method is independent of the employed relay selection policy as long as relay selections in different cooperative frames are independent.

The system consists of a single source node $S$, a destination node $D$, and a set of relay nodes $\mathcal{R} = \{r_1, r_2, \ldots, r_R\}$ where $|\mathcal{R}| = R$. Figure 1 shows the cooperative communication system used in this paper. The relay nodes are pure relay stations and do not inject traffic into the system. All the nodes operate in half-duplex mode, that is, they cannot transmit and receive the information simultaneously. The cooperative transmission paradigm from $S$ to $D$ is a two-phase transmission protocol that is widely used in cooperative wireless networks [3,4,26,27]. In the first phase of communication, $S$ broadcasts a data packet to all the relay nodes by using a fixed amount of power $P_s$ while the relay nodes and the destination are listening. In the second phase, one of the relay nodes who has successfully received the packet in the first phase will be selected by node $D$ (which is also acting as the network controller) to forward the packet to $D$. We call the two phases of transmission of a packet as a *transmission frame*. The relay nodes work in DF mode [4]. In DF mode, a relay node receives the broadcast signal from $S$, detects it and then encodes again, and transmits it to node $D$. All the transmissions from each relay node $i$, $1 \leq i \leq R$, are performed by a fixed amount of power $P_i$. All the links in the system are assumed to be slow Rayleigh fading channels with additive white Gaussian noise. On the basis of the channel quality of the direct link from $S$ to $D$, we may consider two cases for this system. In fact, when the quality of this link is very poor, that is, it has poor average SNR (e.g., when the user is very far from the base station), then the cooperative system is designed such that node $D$ just detects the signal in the second phase of cooperation. When the quality of this link is good enough, node $D$ makes a combination of the received signals in the first and the second phases (e.g., by using MRC or other combining methods) of cooperation to create a stronger signal. These cases are quite well studied and well understood in the cooperative communication literature, for example, [2,4,8,9,26,27].

*Case 1: system without combining*. In the first case, the channel quality between $S$ and $D$ is poor. Therefore, $D$ does not keep the received signal transmitted by the source in the first phase for the purpose of combining. In this case, if $X_S$ denotes the transmitted signal from the source in the first phase, the received signal at each relay node $i$ will be

$$Y_{r_i} = \frac{h_{S-r_i}}{d_{S-r_i}^{\frac{a}{2}}} X_S + Z_i, \qquad \forall i = 1, \ldots, R \tag{1}$$

In (1), $Y_{r_i}$ denotes the received signal at relay node $i$. $h_{S-r_i}$ is the Rayleigh channel coefficient, $d_{S-r_i}$ is the distance between source node $S$ and relay node $i$, $a$ is the path loss exponent, and $Z_i$ denotes the additive zero mean

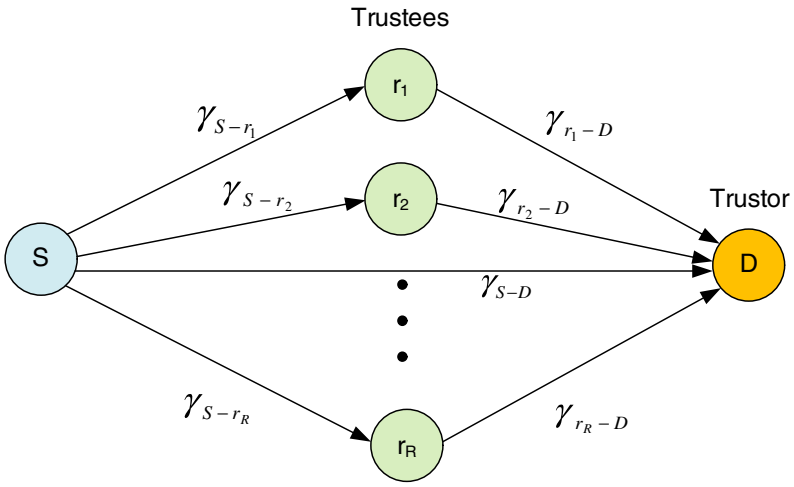



**Figure 1.** The cooperative communication model.

Gaussian noise at relay $i$. Similarly, if $X_i$ denotes the transmitted signal from relay $i$ in the second phase, the received signal at the destination will be

$$Y_D = \frac{h_{r_i-D}}{d_{r_i-D}^{\frac{a}{2}}} X_i + Z_D, \qquad \forall i = 1, \ldots, R. \tag{2}$$

where $Y_D$ denotes the received signal at node $D$. $h_{r_i-D}$ is the Rayleigh channel coefficient, $d_{r_i-D}$ is the distance between relay node $i$ and $D$, and $Z_D$ denotes the additive zero mean Gaussian noise at node $D$.

*Case 2: system with combining*. In the second case, the direct link between $S$ and $D$ has an acceptable quality of channel. Despite the first case, in the second case, $D$ always keeps the received signal in the first phase of transmission to perform diversity combining at the end of a transmission frame. Other settings discussed earlier for the first case of the model are valid for the second case as well. Note that the received signals at the destination in the first and the second phases of transmission are the following.

$$Y_{1D} = \frac{h_{S-D}}{d_{S-D}^{\frac{a}{2}}} X_S + Z_D \tag{3}$$

$$Y_{2D} = \frac{h_{r_i-D}}{d_{r_i-D}^{\frac{a}{2}}} X_i + Z_D, \qquad \forall i = 1, \ldots, R \tag{4}$$

In (3) and (4), $Y_{1D}$ and $Y_{2D}$ are the received signals from direct link $S - D$ and link $r_i - D$, respectively. $h_{S-D}$ and $h_{r_i-D}$ are fading coefficients of links $S - D$ and $r_i - D$, respectively. $d_{S-D}$ and $d_{r_i-D}$ represent the distance from $S$ to $D$ and from relay $i$ to $D$, respectively. Let us denote the instantaneous signal to noise ratio (SNR) of $S - r_i$, $r_i - D$ and $S - D$ links by $\gamma_{S-r_i}$, $\gamma_{r_i-D}$ and $\gamma_{S-D}$, respectively. We assume that the noise power in the transmission spectrum is $W$. We denote the transmission power of source node $S$ and relay node $i$ by $P_S$, and $P_i$, respectively. Thus, we have the following equations for instantaneous SNRs.

$$\gamma_{S-r_i} = \frac{|h_{S-r_i}|^2 P_S}{d_{S-r_i}^a W} \tag{5a}$$

$$\gamma_{r_i-D} = \frac{|h_{r_i-D}|^2 P_i}{d_{r_i-D}^a W} \tag{5b}$$

$$\gamma_{S-D} = \frac{|h_{S-D}|^2 P_S}{d_{S-D}^a W} \tag{5c}$$

As we explained earlier, $D$ also carries out the role of the network controller (network controller is usually the base station or an access point in wireless relaying networks) and performs the relay selection process in the network. In other words, $D$ employs a relay selection policy in which it selects an appropriate relay node on the basis of the available instantaneous channel state information of the system.[†] We assume that relay selection in each frame is performed independent of relay selections in the previous or future frames. Although this assumption seems to be restrictive, such a class of policies is discussed and has been widely used in cooperative communication research [26–28].

*Maximum SNR relay selection policy*: in our cooperative system, we will use maximum SNR policy as the relay selection policy [26,27]. As mentioned earlier, during the first phase of communication, $S$ broadcasts a packet to the relay nodes. Among them, those who have SNR greater than a *threshold* SNR, $\gamma_{\text{thr}}$, can detect the signal correctly. Suppose that when a relay node detects a packet correctly, it broadcasts an instantaneous ACK. Let $\Omega$ denote the set of relay nodes who have detected the packet correctly. Afterwards, node $D$ chooses a relay node $r^*$ whose $\gamma_{r_i-D}$ is the maximum, that is,

$$r^* = \arg \max_{r_i \in \Omega} \gamma_{r_i-D} \tag{6}$$

Relay $r^*$ then transmits the received packet to $D$.

The value of $\gamma_{\text{thr}}$ depends on the acceptable Bit Error Rate (BER) for the application running on the network and also the applied modulation and coding schemes. For example, for voice and video, the acceptable BER ($10^{-3} - 10^{-6}$) is different from what is needed for file transfer ($10^{-6} - 10^{-9}$). The BER–SNR curve is also different for different modulation and coding schemes [20]. Thus, on the basis of the application, the modulation, and coding schemes, the threshold SNR is determined. Here, we assume that the system is using binary phase-shift keying (BPSK) modulation without coding and the acceptable BER is $10^{-6}$.

For detection at $D$ in the case without combining (case 1), $D$ simply decodes $Y_D$. In the second case, $D$ will further use MRC at the destination to combine two received signals from $r^*$ and $S$, that is, $Y_{1D}$ and $Y_{2D}$ [20]. If $D$ can detect the packet correctly, it broadcasts an instantaneous ACK, and the source node erases the packet from its queue. Otherwise, it broadcasts a NACK, and the source retransmits the packet in the next frame of transmission. We assume that all the ACK and NACK packets are very small packets and are sent through separate control channels. Note that because these packets are very small, the amount of spectrum dedicated to control channels is negligible with respect to the spectrum dedicated to the data packets.

We model the maliciousness of each relay node $i$ by a binary random variable $Q_i$ with parameter $q_i$. In other words, we assume that at each transmission frame, any malicious relay node $i$ selected to relay a packet to the destination behaves anomalously and does not forward

[†]In this paper, by channel state information, we mean the instantaneous signal to noise ratio of all the links in the system. It is assumed that the channel state information is estimated at the receiver of each communication link by using the existing channel estimation methods.

the packet with probability $q_i$. Stochastic modeling of the maliciousness of a node has been appeared previously in the literature, for example, [12,15,29]. In fact, a clever attacker may use stochastic malicious behavior in which it tries to hide its maliciousness for a longer time [29].

In this paper, our purpose is to derive a trust value corresponding to each relay node. The trust value must be an estimate of the complement of the expected value of the maliciousness random variable (i.e., $1 - q_i$). To this end, we use Bayesian framework and perform iterative observations of the system including the channel conditions, relay selections, and the net amount of packets received and forwarded by each relay node. We will discuss about the iterative observation of the system in the following section in detail. On the basis of these observations, we will derive a trust value for each relay node after each observation iteration.

# 4. BACKGROUND

## 4.1. Trust and trustworthiness

Various definitions for trust have been used in different areas of science. For our purposes, *trust level* can be defined as the degree of belief about the behavior of another entity [30]. The trust level associated with an entity may be interpreted in two different ways. *Trust* refers to subjective aspect of the trust level, whereas *trustworthiness* refers to the objective aspect of the trust level. In general, trust is the probability of the event that an entity behaves as expected. We use the term *trustor* for the entity that is going to trust some other entities for a cooperation and the term *trustee* for the one that is going to be trusted on for the cooperation. What trustor should do is to estimate a level of trust for any trustee. If the trustor ignores the gap between trustworthiness and trust, there will be a miscalculation of the involved risk. By misplacing trust, either the trustor looses the opportunity to cooperate with the trustees or the risk of deceit increases. Thus, we should minimize the difference between the calculated trust and the trustworthiness [31]. In the model described in Section 3, node $D$ (i.e., the destination nodes that is also acting as the network controller and manages the cooperation process in the system) is the trustor, and the relay nodes are the trustees. In fact, $D$ as the trustor expects a relay node to forward the received packet whenever it is selected to do so and the channel is in good condition.

## 4.2. Bayesian methodology

Bayesian methodology is an approach that is well suited for stochastic problems of the type we wish to address. The following is a brief review of this methodology along with an example. In Section 5, we will demonstrate that this methodology needs to be extended to be applied effectively to our cooperative system.

Consider a single node $R$ acting as a relay node (or router) in a network. Node $R$ receives data packets from an upstream sender namely $S$ and then forwards them to a downstream receiver namely $D$. In this example, node $D$ is the trustor whose goal is to obtain a trust value for relay node $R$. If node $R$ behaves maliciously, it discards some of the received packets and does not forward them to $D$. We model the maliciousness by a Bernoulli random variable with parameter $q$, and therefore, $R$ discards a packet with probability $q$ independent of other transmissions. To such a node, a *trust* value $T$ from the interval $[0, 1]$ is associated, which is an estimate of the parameter $\bar{q} = 1 - q$, that is, the unknown parameter to the trustor. The goal of the trustor then would be to obtain an estimate of $\bar{q}$. Note that, the trustor does not have any information about $\bar{q}$, and therefore, this parameter is a random variable in its point of view. Specifically, it can summarize its belief about $\bar{q}$ in a probability distribution assuming that $\bar{q}$ follows a prior distribution. Thus, at the beginning when there is no observation from the system, the trustor assumes that $\bar{q}$ follows a prior distribution (later we will see that this prior distribution is a uniform distribution). It then updates this distribution by performing iterative observations on the system, that is, counting the number of packets entering node $R$ from $S$ and the number of forwarded packets by $R$ to $D$. These numbers are obtained iteratively with a fixed predetermined iteration period. Note that the number of packets forwarded from node $R$ to $D$ is known for $D$. The number of packets entering node $R$ from $S$ is kept by $S$ and then at the end of each iteration will be forwarded to $D$. Note that this is not a feedback or loop in the system. This is just a simple message exchange from $D$ to $S$, which is done iteratively and helps $D$ to compute the trust values for the relay node $R$. We assume that the security and integrity of all the information exchanges are guaranteed by applying cryptographic techniques such as encryption/decryption algorithms (e.g., Advanced Encryption Standard (AES)), authentication protocols (e.g., adaptive and lightweight protocol for hop-by-hop authentication [32,33], hash chains and Merkle trees [34], and counter mode with cipher block chaining message authentication code protocol [35]). Examples of existing security protocols in wireless networks is the Wi-Fi protected access protocol, which contains the following components: 802.1X for authentication, robust secure network for keeping track of associations, and AES-based cipher block chaining message authentication code protocol to provide confidentiality, integrity, and data origin authentication [35]. Although this protocol was proposed as a security protocol for IEEE 802.11i, the same protocol with some modifications can be applied in cooperative wireless networks [35]. In this paper, we assume that all the communications in the network are secure and the goal of a malicious (or compromised) relay node is just to ruin the performance of the network by discarding the received packets from $S$.

At the beginning, when there is no available observation on the system, the trustor assumes that $\bar{q}$ follows a uniform

distribution (the prior distribution at iteration $t = 0$). Each time the trustor makes an observation at iteration $t \in \mathbb{N}$, it can derive the posterior distribution of $\bar{q}$ at that time on the basis of the prior distribution of $\bar{q}$ at iteration $t-1$ and the current observation at iteration $t$. It then uses the obtained posterior distribution as the prior distribution at iteration $t+1$, and this procedure continues. The expected value of $\bar{q}$ with respect to the obtained posterior distribution after the observation of iteration $t$ is called the trust value at iteration $t$ [12,15,23,24].

Suppose that the trustor observes the system iteratively, and during each iteration $t$, it observes $k(t)$ packets received by $R$ and $\ell(t)$ packets transmitted successfully by $R$. Let $L(t)$ and $K(t)$ denote the random variables corresponding to the number of packets transmitted successfully by $R$ and the the number of packets received by $R$, respectively. Also, assume that $D$ can summarize its belief about the random variable $\bar{q}$ in a prior distribution $f_{t-1}(\bar{q})$. Having $k(t)$, $\ell(t)$, and $f_{t-1}(\bar{q})$, node $D$ can derive the posterior distribution of random variable $\bar{q}$ via Bayes' rule as follows.

$$f_t(\bar{q}) = \frac{P(L(t) = \ell(t) \mid \bar{q}, K(t) = k(t))\, f_{t-1}(\bar{q})}{\int_0^1 P(L(t) = \ell(t) \mid \bar{q}, K(t) = k(t))\, f_{t-1}(\bar{q})\, d\bar{q}} \tag{7}$$

On the basis of our assumption about the malicious behavior of relay $R$, the random variable $L(t)$ given $\bar{q}$ and $K(t)$ follows a binomial distribution, that is,

$$\begin{aligned} &P(L(t) = \ell(t) \mid \bar{q}, K(t) = k(t)) \\ &\quad = \binom{k(t)}{\ell(t)} \bar{q}^{\ell(t)} q^{k(t)-\ell(t)} \end{aligned} \tag{8}$$

As binomial and Beta distributions are conjugate distributions, one can easily derive the distribution function of $\bar{q}$ as follows. At the beginning (iteration $t = 0$), $D$ has no information about the distribution of $\bar{q}$. Therefore, it assumes that $\bar{q}$ follows a uniform distribution in the interval $[0, 1]$ with mean 0.5.

$$f_0(\bar{q}) = U(0, 1) = \text{Beta}(\alpha(0), \beta(0)) = \text{Beta}(1, 1) \tag{9}$$

where

$$\text{Beta}(\alpha, \beta) = \frac{\bar{q}^{(\alpha-1)} q^{(\beta-1)}}{\int_0^1 \bar{q}^{(\alpha-1)} q^{(\beta-1)} d\bar{q}} \tag{10}$$

In (10), $\alpha$ and $\beta$ are two free parameters of Beta distribution. This agrees with intuition because at the beginning, there is no evidence about the maliciousness of $R$. Therefore, $D$ may assume that $R$ is malicious with probability 0.5. It is shown in [12] that if $f_{t-1}(\bar{q}) = \text{Beta}(\alpha(t-1), \beta(t-1))$, given $K(t) = k(t)$ and $L(t) = \ell(t)$ for all $t \geq 1$, we have

$$f_t(\bar{q}) = \text{Beta}(\alpha(t-1) + \ell(t), \beta(t-1) + k(t) - \ell(t)) \tag{11}$$

In other words, $f_t(\bar{q})$ follows $\text{Beta}(\alpha(t), \beta(t))$ distribution with the parameters

$$\begin{aligned} &\alpha(t) = \alpha(t-1) + \ell(t), && \alpha(0) = 1 \\ &\beta(t) = \beta(t-1) + k(t) - \ell(t), && \beta(0) = 1 \end{aligned} \tag{12}$$

Note that Equations (9) and (11) construct a recursive formula by which $D$ can easily update the prior distribution function $f_t(\bar{q})$ without any need to calculate Equation (7) repeatedly.

On the basis of our previous discussion, after the $t$th iteration, trust value is defined as the expected value of $\bar{q}$ with respect to the distribution function $f_t(\bar{q}) = \text{Beta}(\alpha(t), \beta(t))$, that is,

$$T(t) = \frac{\alpha(t)}{\alpha(t) + \beta(t)} \tag{13}$$

This is because the expected value of a Beta random variable with parameters $\alpha$ and $\beta$ equals $\frac{\alpha}{\alpha+\beta}$. Therefore, at the beginning (iteration $t = 0$) when there is no observation available, the trust is equal to $T(0) = \frac{\alpha(0)}{\alpha(0)+\beta(0)} = 0.5$, and then after obtaining the first observation we have $T(1) = \frac{\alpha(1)}{\alpha(1)+\beta(1)}$, where $\alpha(1) = 1 + \ell(1)$ and $\beta(1) = 1 + k(1) - \ell(1)$. This procedure continues, and after each iteration, $D$ obtains the trust value associated to the relay node $R$ at that iteration according to (13). Note that as time proceeds, $D$ will have more iterations and more observations about the behavior of $R$, and therefore, it can obtain a more precise estimate of trust.

It is worth mentioning that more than one stream of data may be passed through node $R$ from different upstream traffic sources (because of routing different traffic flows through $R$). Therefore, $D$ may observe different observations about the malicious behavior of $R$ with respect to each stream. In such a case, a weighted sum of the computed trusts for each stream can be used as an estimate of $R$'s trust value.

The Bayesian framework described earlier is a general framework to estimate the distribution of an unknown parameter of a process by using observations [23,24]. In fact, if we can model a process in a system with a Bernoulli process (independent successes and failures) with unknown probability of success, Bayesian methodology can be used to obtain an estimate of the unknown probability as the mean of the prior conjugate distribution, which is a Beta distribution function.

## 5. TRUST ESTABLISHMENT FOR WIRELESS RELAYING NETWORKS

In this section, we propose a trust establishment scheme for cooperative relaying networks based on Bayesian framework described in the previous section.

### 5.1. Motivation

In the cooperative system described in section 3, not all of the unsuccessful packet transmissions from a relay node are due to maliciousness of that node. They might also be the result of unreliability of channels. Therefore, by using the Bayesian framework solely based on the number of received and successfully forwarded packets, we cannot obtain an accurate derivation of trust values. In other words, the obtained trust values would not be pure trust values and will be biased. The following example clarifies this fact.

*Example:* consider a simple cooperative system with four nodes. Source node 1 generates traffic and transmits the traffic to node 4 via cooperation with nodes 2 and 3 (Figure 2). The transmission protocol is a two-phase protocol similar to what discussed in Section 3. The channels between source node 1 and relay nodes 2 and 3 are perfect noise free channels. Among nodes 2 and 3, one of them is selected randomly (with probability 0.5) to forward the packet to destination node 4. The channel between relay node 2 and destination node 4 is modeled by a binary erasure channel with success probability of 0.95, and the channel between relay node 3 and destination node 4 is modeled by another binary erasure channel with success probability of 0.65. Relay 2 is malicious with probability 0.35, and relay node 3 is malicious with probability 0.2. Using the Beta function trust establishment scheme discussed in the previous section, we obtained the trust values through simulations in Matlab. We have assumed that each iteration consists of 100 transmission frames. We expect the trust of relays 2 and 3 to be 0.65 and 0.8, respectively. As we explained before, each frame consists of two transmission phases. In the first phase, node 1 broadcasts its information to nodes 2 and 3. In the second phase, one of the nodes 2 and 3 is selected (by node 4, which is assumed to be network controller) with probability 0.5 to forward the received packet.

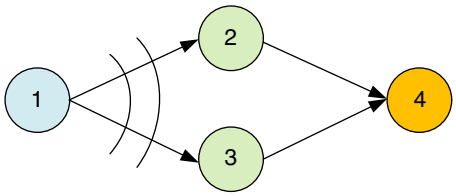



**Figure 2.** The cooperative model of the example.

In the first example, we run the simulation for 400 iterations (i.e., 40 000 transmission frames). As we can see in Figure 3(a), the conventional Bayesian trust establishment gives inaccurate trust values with inverse order rather than what we expect (it computes 0.475 for relay 2 and 0.425 for relay 3). Although relay 2 is more malicious than relay 3, it has a larger connectivity probability and subsequently, more successfully transmitted packets than relay 3. Therefore, using conventional Bayesian methodology, we achieve a larger trust value for relay 2 than for relay 3. In fact, the obtained trust values are biased by the channel conditions.

Consider another example where the success probability of the channel between node 2 and destination node 4 is 0.65 and the success probability of the channel between node 3 and destination is 0.85. Suppose that nodes 2 and 3 are initially malicious with probabilities 0.55 and 0.2, respectively. After iteration 150, node 3 changes its maliciousness to 0.6. We run the simulation for longer time, that is, 1500 iterations (150 000 transmission frames) as our goal is to observe the accuracy of trust tracking in the cases where malicious behavior of a node changes rapidly. Figure 3(b) shows the trust tracking of the system by using the conventional Bayesian trust establishment described in the previous section. Before iteration 150, we expect the trust of relays 2 and 3 to be 0.45 and 0.8, respectively, but it returns inaccurate results of 0.25 and 0.5, respectively. After the maliciousness of relay node 3 changes from 0.2 to 0.6, the trust of relay 3 should change to 0.4, that is, less than the trust of relay 2, which is 0.45. By using the conventional Bayesian method, computed trusts at the end

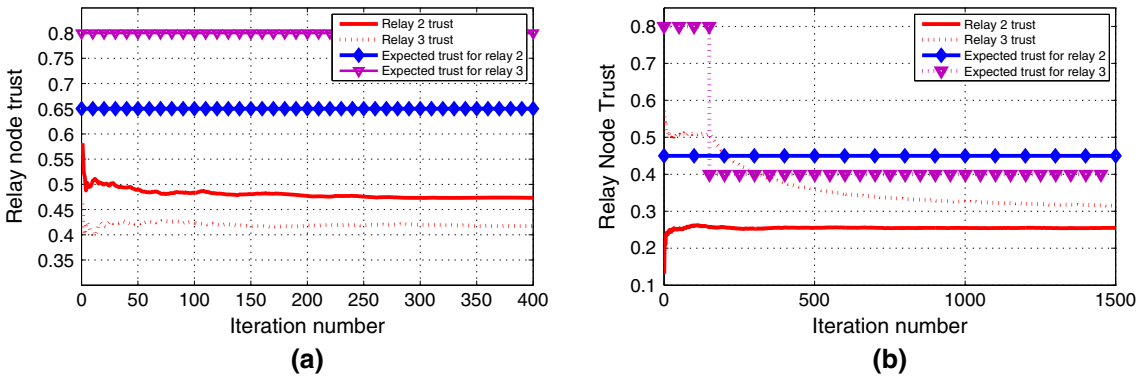



**Figure 3.** Conventional Bayesian trust establishment in a simple cooperative system. It is observed that the conventional Bayesian trust establishment fails to achieve accurate trust values for the relay nodes.

of the simulation are 0.25 for relay 2 and 0.32 for relay 3. Importantly, this method gives us the inverse ranking of trusts after changing the maliciousness of node 3. In other words, although this method tries to track the trust after iteration 150, the starting and ending points of this tracking are not correct. Again, not considering the channel connectivity probabilities and relay selection probabilities in trust establishment is problematic. We will see similar results for more realistic channel conditions and relay selection policies in Section 6.

### 5.2. Proposed trust establishment for cooperative relaying networks

The problems with the application of conventional Bayesian approach in cooperative wireless networks mentioned in the previous part of this section motivate us to introduce a trust establishment scheme for the two cases of the cooperative system (i.e., with combining and without combining) described in Section 3. In our scheme, the goal is to obtain an accurate trust value corresponding to each relay node. In other words, the destination $D$ that manages the relay selection in the system should be able to obtain an accurate trust value for each relay node. It can use these trust values to decide whether a relay node is trustworthy or not and later take the proper action or remove a relay node from its list of reliable relay nodes if its associated trust value drops below a specific threshold. In this paper, our focus would be on the derivation of trust values, and the application of those values is out of the scope of this paper. We will consider both the cases of the cooperative system described in Section 3 for each of which we will introduce the proposed trust establishment scheme. We use superscripts 1 and 2 for the variables associated to cases 1 and 2 of the system, respectively.

As explained earlier, trust establishment is usually based on iterative monitoring of the system. At each iteration $t$, the trustor (which is node $D$) counts the number of successful transmissions from $S$ to each relay node $i$. It can count this number by using the number of ACKs broadcast from relay $i$. Let $k_i^{(1)}(t)$ and $k_i^{(2)}(t)$ denote this number for cases 1 and 2 of the system, respectively. The total number of successful transmissions from relay $i$ to $D$ is also counted. These numbers depend on the maliciousness of the relay node $i$ as well as channel conditions and the relay selection policy. Suppose that $D$ observes $\ell_i^{(j)}(t)$ successful transmission from relay $i$ to $D$ at iteration $t$ in case $j = 1, 2$. According to (12) and (13) and by using the conventional Bayesian trust establishment, $D$ computes the trust of relay node $i$ at iteration $t$ for case $j = 1, 2$ as follows.

$$T_i^{(j)}(t) = \frac{\alpha_i^{(j)}(t)}{\alpha_i^{(j)}(t) + \beta_i^{(j)}(t)}, \quad i \in \mathcal{R}\ ,\ t \in \mathbb{Z}^+ \tag{14}$$

where

$$\begin{aligned} \alpha_i^{(j)}(t) &= \alpha_i^{(j)}(t-1) + \ell_i^{(j)}(t), & \alpha_i^{(j)}(0) &= 1 \\ \beta_i^{(j)}(t) &= \beta_i^{(j)}(t-1) + k_i^{(j)}(t) - \ell_i^{(j)}(t), & \beta_i^{(j)}(0) &= 1 \end{aligned} \tag{15}$$

The amount of $\alpha_i^{(j)}(t)$ not only depends on the maliciousness of relay node $i$ but also depends on the number of times that the relay was selected for cooperation. It is also dependent to the channel conditions. Therefore, the obtained trust values in (14) are biased on the channel conditions and the relay selection policy. We attempt to remove this bias by modifying the trust value in (14). Let $\Theta_i^{(j)}$ (for case $j = 1, 2$) represent the event that relay node $i$ is selected by $D$ according to an employed relay selection policy, for example, maximum SNR policy described in Section 3. Therefore for cases 1 and 2 , we can obtain the accurate trust values $T_i^{(1)}(t)$ and $T_i^{(2)}(t)$ as follows.

$$T_i^{(1)}(t) = \frac{\alpha_i^{(1)}(t)}{\alpha_i^{(1)}(t) + \beta_i^{(1)}(t)} \cdot \frac{1}{P(\gamma_{r_i-D} \geq \gamma_{\text{thr}})} \cdot \frac{1}{P\left(\Theta_i^{(1)} \mid \gamma_{r_i-D} \geq \gamma_{\text{thr}}, \gamma_{S-r_i} \geq \gamma_{\text{thr}}\right)} \tag{16}$$

$$T_i^{(2)}(t) = \frac{\alpha_i^{(2)}(t)}{\alpha_i^{(2)}(t) + \beta_i^{(2)}(t)} \cdot \frac{1}{P(\gamma_{r_i-D} + \gamma_{S-D} \geq \gamma_{\text{thr}})} \cdot \frac{1}{P\left(\Theta_i^{(2)} \mid \gamma_{r_i-D} + \gamma_{S-D} \geq \gamma_{\text{thr}}, \gamma_{S-r_i} \geq \gamma_{\text{thr}}\right)} \tag{17}$$

The intuition behind these two formulas is that other than maliciousness of relay node $i$, there are two other factors that make a packet fail to reach the destination. One is the quality of the communication channels in the second phase of transmission, and the other one is that relay $i$ may not be selected for cooperation. By applying the Bayes' rule, we can obtain Equations (16) and (17). Note that the destination does not know the statistics of relay selections and also the channel conditions. Therefore, the destination follows the same estimation approach (Bayesian methodology) to obtain the values of $P\left(\gamma_{r_i-D} \geq \gamma_{\text{thr}}\right)$, $P\left(\Theta_i^{(1)} \mid \gamma_{r_i-D} \geq \gamma_{\text{thr}}, \gamma_{S-r_i} \geq \gamma_{\text{thr}}\right)$, $P(\gamma_{r_i-D} + \gamma_{S-D} \geq \gamma_{\text{thr}})$, and $P\left(\Theta_i^{(2)} \mid \gamma_{r_i-D} + \gamma_{S-D} \geq \gamma_{\text{thr}}, \gamma_{S-r_i} \geq \gamma_{\text{thr}}\right)$. In other words, given the independence of relay selection decisions in different frames, we can model the selection of relay $i$ given the events $\gamma_{S-r_i} \geq \gamma_{\text{thr}}$ and $\gamma_{r_i-D} \geq \gamma_{\text{thr}}$ in case 1 and the selection of relay $i$ given the events $\gamma_{S-r_i} \geq \gamma_{\text{thr}}$ and $\gamma_{r_i-D} + \gamma_{S-D} \geq \gamma_{\text{thr}}$ in case 2 as two Bernoulli random variables with parameters $p_{\Theta_i}^{(1)}$ and $p_{\Theta_i}^{(2)}$, respectively. Assume that $\ell_{\Theta_i}^{(1)}(t)$ represents the number of times that relay $i$ is selected at

iteration $t$ in case 1 given both $\gamma_{S-r_i}$ and $\gamma_{r_i-D}$ are greater than the threshold SNR. Also assume that $k^{(1)}_{\Theta_i}(t)$ denotes the number of times at iteration $t$ that both $\gamma_{S-r_i}$ and $\gamma_{r_i-D}$ are greater than the threshold SNR. Similarly, assume that $\ell^{(2)}_{\Theta_i}(t)$ represents the number of times that relay $i$ is selected at iteration $t$ in case 2 given both $\gamma_{S-r_i}$ and $\gamma_{r_i-D}+\gamma_{S-D}$ are greater than the threshold SNR. Also assume that $k^{(2)}_{\Theta_i}(t)$ denotes the number of times at iteration $t$ that both $\gamma_{S-r_i}$ and $\gamma_{r_i-D}+\gamma_{S-D}$ are greater than the threshold SNR. Given $\ell^{(1)}_{\Theta_i}(t), \ell^{(2)}_{\Theta_i}(t), k^{(1)}_{\Theta_i}(t)$, and $k^{(2)}_{\Theta_i}(t)$, the parameter $p^{(1)}_{\Theta_i}$ in case 1 follows a Beta distribution Beta $\left(\alpha^{(1)}_{\Theta_i}(t), \beta^{(1)}_{\Theta_i}(t)\right)$, and $p^{(2)}_{\Theta_i}$ in case 2 follows a Beta distribution Beta $\left(\alpha^{(2)}_{\Theta_i}(t), \beta^{(2)}_{\Theta_i}(t)\right)$ at iteration $t$, and their corresponding means are the following.

$$\frac{\alpha^{(j)}_{\Theta_i}(t)}{\alpha^{(j)}_{\Theta_i}(t)+\beta^{(j)}_{\Theta_i}(t)} \qquad j=1,2 \tag{18}$$

where

$$\begin{aligned}
&\alpha^{(j)}_{\Theta_i}(t)=\alpha^{(j)}_{\Theta_i}(t-1)+\ell^{(j)}_{\Theta_i}(t) && \alpha^{(j)}_{\Theta_i}(0)=1\\
&\beta^{(j)}_{\Theta_i}(t)=\beta^{(j)}_{\Theta_i}(t-1)+k^{(j)}_{\Theta_i}(t)-\ell^{(j)}_{\Theta_i}(t) && \beta^{(j)}_{\Theta_i}(0)=1
\end{aligned} \tag{19}$$

This result is a direct application of Bayesian framework (refer to Section 4.2) in estimating $P\left(\Theta^{(1)}_i \mid \gamma_{r_i-D}\geq\gamma_{\text{thr}}, \gamma_{S-r_i}\geq\gamma_{\text{thr}}\right)$ and $P\left(\Theta^{(2)}_i \mid \gamma_{r_i-D}+\gamma_{S-D}\geq\gamma_{\text{thr}}, \gamma_{S-r_i}\geq\gamma_{\text{thr}}\right)$. The same argument is used to estimate $P\left(\gamma_{r_i-D}\geq\gamma_{\text{thr}}\right)$ and $P\left(\gamma_{r_i-D}+\gamma_{S-D}\geq\gamma_{\text{thr}}\right)$, that is, given the independence of channel states in different frames, these two events are modeled by two Bernoulli random variables whose parameters $p^{(1)}_{\gamma_i}$ and $p^{(2)}_{\gamma_i}$ follow Beta distribution at each iteration. Specifically in case 1, if $D$ observes that the SNR of link $r_i-D$ is greater than the threshold in $\ell^{(1)}_{\gamma_i}(t)$ cases out of $k^{(1)}_{\gamma_i}(t)$, and in case 2, if it observes that $\gamma_{r_i-D}+\gamma_{S-D}\geq\gamma_{\text{thr}}$ in $\ell^{(2)}_{\gamma_i}(t)$ cases out of $k^{(2)}_{\gamma_i}(t)$, then $p^{(j)}_{\gamma_i}$ given $\ell^{(j)}_{\gamma_i}(t)$ and $k^{(j)}_{\gamma_i}(t)$ follows a Beta distribution Beta $\left(\alpha^{(j)}_{\gamma_i}(t), \beta^{(j)}_{\gamma_i}(t)\right)$, $j=1,2$, where

$$\begin{aligned}
&\alpha^{(j)}_{\gamma_i}(t)=\alpha^{(j)}_{\gamma_i}(t-1)+\ell^{(j)}_{\gamma_i}(t), && \alpha^{(j)}_{\gamma_i}(0)=1\\
&\beta^{(j)}_{\gamma_i}(t)=\beta^{(j)}_{\gamma_i}(t-1)+k^{(j)}_{\gamma_i}(t)-\ell^{(j)}_{\gamma_i}(t), && \beta^{(j)}_{\gamma_i}(0)=1
\end{aligned} \tag{20}$$

with mean

$$\frac{\alpha^{(j)}_{\gamma_i}(t)}{\alpha^{(j)}_{\gamma_i}(t)+\beta^{(j)}_{\gamma_i}(t)} \tag{21}$$

We use this value with $j=1$ as the estimate of $P(\gamma_{r_i-D}\geq\gamma_{\text{thr}})$ for case 1 and with $j=2$ as the estimate of $P\left(\gamma_{r_i-D}+\gamma_{S-D}\geq\gamma_{\text{thr}}\right)$ for case 2 at iteration $t$.

According to (16), (17), (18), and (21), we can then formulate the trust at each iteration $t$ as

$$T^{(j)}_i(t)=\frac{\alpha^{(j)}_i(t)}{\alpha^{(j)}_i(t)+\beta^{(j)}_i(t)}\cdot\frac{\alpha^{(j)}_{\Theta_i}(t)+\beta^{(j)}_{\Theta_i}(t)}{\alpha^{(j)}_{\Theta_i}(t)}\cdot\frac{\alpha^{(j)}_{\gamma_i}(t)+\beta^{(j)}_{\gamma_i}(t)}{\alpha^{(j)}_{\gamma_i}(t)} \tag{22}$$

where the parameters $\alpha^{(j)}_i(t)$, $\beta^{(j)}_i(t)$, $\alpha^{(j)}_{\Theta_i}(t)$, $\beta^{(j)}_{\Theta_i}(t)$, $\alpha^{(j)}_{\gamma_i}(t)$, and $\beta^{(j)}_{\gamma_i}(t)$ for $j=1,2$ (cases 1 and 2) are updated at each iteration $t$ according to (15), (19), and (20).

Note that in the proposed trust establishment scheme, we are using the existing information at the relay selection process. Therefore, our scheme does not impose communication overhead to the system for monitoring and measurements. It is worth mentioning that the proposed method is independent of the *employed* relay selection policy and similar results can be drawn for other relay selection policies with independent decisions in different transmission frames. Examples of other relay selection policies can be found in [28,36–39].

## 6. SIMULATION RESULTS AND DISCUSSIONS

In this section, we present the simulation results to show the effectiveness of the proposed trust establishment method. We used Matlab to develop the simulation environment in all the experiments. The topology used in the first part of the simulations is the same as Figure 1 with one source node, one destination, and four relay nodes. In the first part of the simulations, we are intended to verify the effectiveness of the proposed trust establishment method in (22) for cases 1 and 2 of the cooperative system in Figure 1. The system is using BPSK modulation without any coding scheme, and the channels are slow Rayleigh fading channels. We assume that during each packet transmission frame, the fading coefficients are fixed. Moreover, we assume that the nodes are not mobile. We will consider mobility in the second part of our simulations. Because the variations of a channel are modeled by Rayleigh random variables, the SNR corresponding to that channel follows exponential distribution. Thus, in the simulations, we model the SNRs by exponential random variables. We have assumed that the acceptable BER is $10^{-6}$ requiring the minimum SNR of 54 dB to achieve this BER for BPSK. As a result, the threshold SNR would be $\gamma_{\text{thr}}=54$ dB. Assume that the relays act maliciously with probabilities $0.1, 0.2, 0.3$, and $0.4$, that is, $E[Q_1]=0.1$, $E[Q_2]=0.2$, $E[Q_3]=0.3$, and $E[Q_4]=0.4$. These numbers are chosen arbitrarily. The same conclusions can

be drawn for other values as well. We have considered two situations of high and low SNR regimes for cases 1 and 2. In the high and low SNR regimes, the SNRs of links $S - r_i$ and links $r_i - D$, $i = 1, 2, 3, 4$, are exponential random variables with the mean equal to the elements of vectors $(60, 70, 63, 65)$ dB and $(52, 49, 54, 50)$ dB, respectively. These vectors of SNR are chosen arbitrarily. We have tested the proposed trust establishment scheme for other SNR vectors for which we obtained similar performance results. Note that these SNRs for the wireless links are achievable depending on the distance of the wireless link, fading coefficient, and noise power. In case 2, the mean of exponential random variable of SNR for link $S-D$ is assumed to be 50 dB.

In both cases, we considered the two-phase transmission protocol explained in Section 3. The number of frames in an iteration is assumed to be 100 frames, that is, we observe the system every 100 frames to obtain $\alpha_i^{(j)}(t), \beta_i^{(j)}(t), \alpha_{\Theta_i}^{(j)}(t), \beta_{\Theta_i}^{(j)}(t), \alpha_{\gamma_i}^{(j)}(t)$, and $\beta_{\gamma_i}^{(j)}(t)$ in each case $j = 1, 2$. Note that these parameters are obtained in each iteration according to (15), (19), and (20). Duration of simulations is set to 1000 iterations (or equivalently $10^5$ transmission frames).

### 6.1. Case 1: cooperative relaying without combining

In Figures 4 and 5, we compare the trust values of case 1 obtained from the proposed method (Equation (22) for $j = 1$) and the conventional Bayesian trust establishment method (Equation (14)). We expect to obtain trust values 0.9, 0.8, 0.7, and 0.6 for relay nodes 1 to 4, respectively. In these figures, only the trusts of relay nodes 1 and 3 are illustrated for clarity of figures. As shown in both cases, the proposed trust establishment scheme estimates the trust

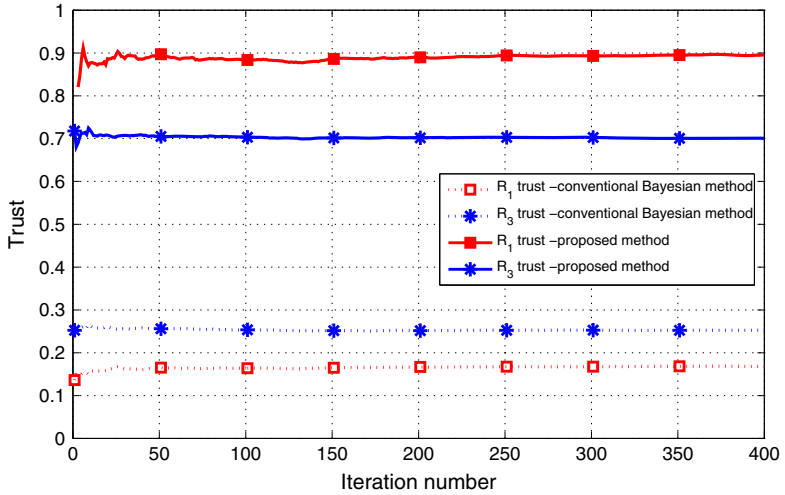



**Figure 4.** Trust establishment in the low signal to noise ratio regime in case 1 (without combining).

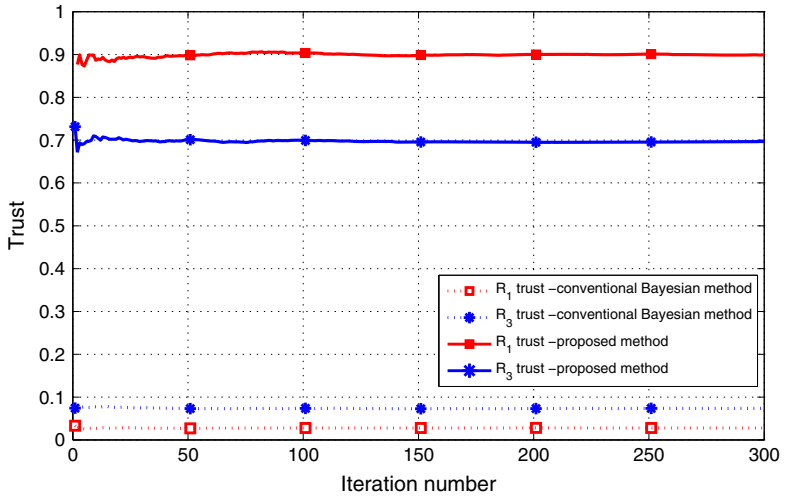



**Figure 5.** Trust establishment in the high signal to noise ratio regime in case 1 (without combining).

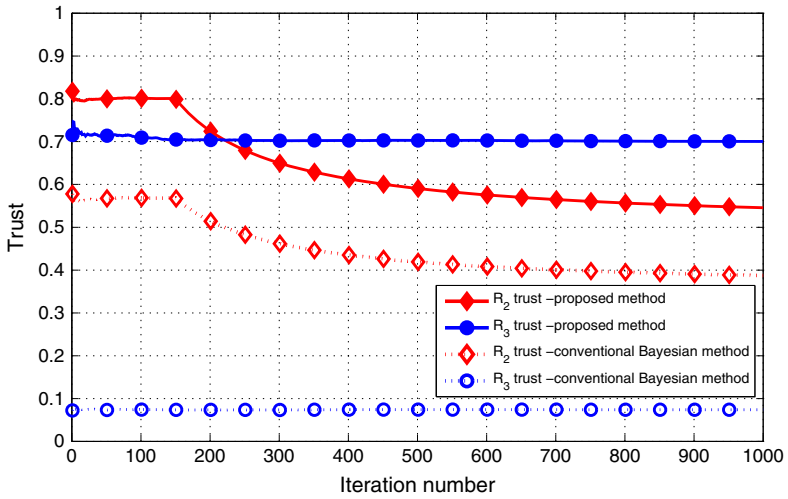



**Figure 6.** Trust tracking with time in case 1 (without combining) in high signal to noise ratio regime.

values of the relay nodes accurately. In contrast, the conventional Bayesian method is biased by channel conditions and the relay selection policy and cannot establish a reliable trust value for the relay nodes. In both figures, we observe that the conventional Bayesian method not only gives incorrect trust values for relay nodes 1 and 3 but also computes the trust of relay 1 below that of relay 3. The reason is that in both cases, relay node 3 has better average channel condition rather than relay 1. Therefore, it is more likely to select relay 3 for cooperation rather than relay 1. It also has a larger probability of successful packet forwarding than relay 1. Because the conventional Bayesian method does not consider the channel condition and relay selection policy in its trust computation process, it fails to calculate accurate and reliable trust values for the relays.

Another point about these two figures is that in low SNR case (Figure 4), the conventional Bayesian method results in better estimates of trust rather than what it does in the high SNR case (Figure 5). The reason is that in low SNR case, in contrast with the high SNR case, the average SNR of relays 1 and 3 is larger than relay nodes 2 and 4. Therefore, the probabilities of selecting relay nodes 1 and 3 are higher than relay nodes 2 and 4 in the low SNR case. Thus, relay nodes 1 and 3 have more opportunity for forwarding the received packets in low SNR case rather than in high SNR case. This is another example of how channel conditions can skew results and expectations.

In another experiment, we simulated the case in which the malicious probability of a relay node suddenly changes at a certain point of time. Starting from the same initial conditions as earleir, we assume that at the 150th iteration, maliciousness of relay node 2 changes to $E[Q_2] = 0.5$. Note that the channel conditions are in the high SNR regime.

In this experiment, we expect the trust of relay node 3 to be 0.7 and the trust of relay 2 to change from 0.8 to 0.5 after iteration 150. This means that we expect to see the trust value of relay 2 falling below that of relay 3 after iteration 150. As we observe from Figure 6, the conventional Bayesian method not only gives incorrect trust estimations before and after iteration 150 but also does not satisfy our expectation about the inversion of the rankings of trusts after iteration 150.

In contrast, Figure 6 shows that the proposed method can track the trust in time accurately. From Figure 6, we can also see that the response of the trust tracking is such that it cannot track rapid changes of trust in the system. This is concluded from the fact that even after 1000 iterations, the trust value of relay 2 cannot reach 0.5. In Figure 6, we observe that after iteration 1000, the trust value is 0.55 and still converging to 0.5. To improve the speed of tracking, we may further introduce a sliding window in the trust computation process at node $D$ as follows. In the computation of trust value at each iteration, $D$ considers only the observations obtained inside a sliding window and discards the observations of the frames before the sliding window. Therefore, in calculation of trust values after the trust change, the effect of previous observations before the trust change is reduced. With a sliding window size of $\omega$ at iteration $t$, Equation (15) is changed to the following.

$$\begin{aligned}
&\alpha_i^{(j)}(t) = \alpha_i^{(j)}(t-1) + \ell_i^{(j)}(t) - \ell_i^{(j)}(t-\omega)\\
&\alpha_i^{(j)}(0) = 1\\
&\beta_i^{(j)}(t) = \beta_i^{(j)}(t-1) + k_i^{(j)}(t) - \ell_i^{(j)}(t)\\
&\qquad\qquad - k_i^{(j)}(t-\omega) + \ell_i^{(j)}(t-\omega)\\
&\beta_i^{(j)}(0) = 1\\
&k_i^{(j)}(\tau) = 0, \quad \ell_i^{(j)}(\tau) = 0, \quad \forall \tau \le 0
\end{aligned} \tag{23}$$

By using Equations (22) and (23), the trust at iteration $t$ is calculated for the window-based approach. Figure 7

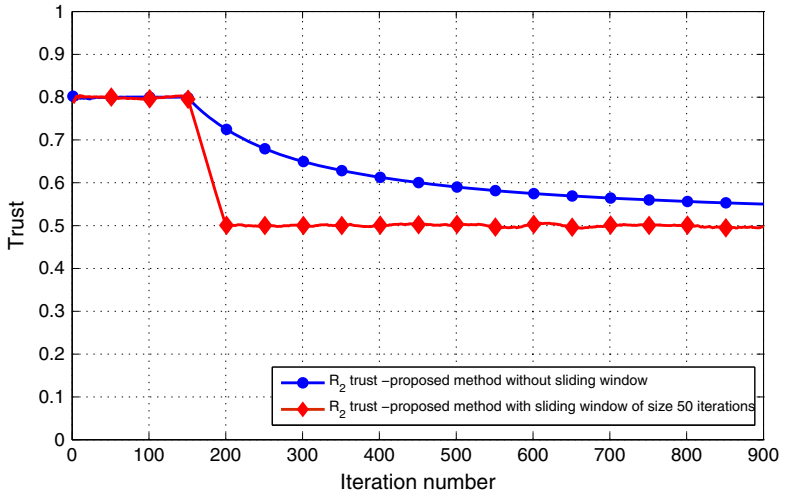



**Figure 7.** Trust tracking with and without using a sliding window in case 1 (without combining) in high signal to noise ratio regime.

compares the trust for the proposed scheme with and without applying the sliding window. In our simulation, we set $\omega$ equal to 50 iterations. It can be inferred from Figure 7 that by applying the sliding window approach trust value of relay 2 converges to 0.5 quickly in 50 iterations from iteration 150 to 200. Therefore, trust tracking is much more faster in the case where a sliding window is used.

Note that selection of an appropriate window size is very important in this case. Selection of a large window size may result in delay in trust change tracking (such as Figure 5 as the extreme case), and selection of a small window size may result in rapid fluctuation of the computed trust.

## 6.2. Case 2: cooperative relaying with combining

In Figures 8 and 9, we compare the trust values of case 2 obtained from the proposed method (Equation (22) for $j = 2$) and the conventional Bayesian trust establishment method (Equation (14)) in high and low SNR regimes. We expect to have trust values 0.9, 0.8, 0.7, and 0.6 for relay nodes 1 to 4, respectively. Only the trusts of two relay nodes are illustrated because of space limitations. As shown in both SNR regimes, the proposed trust establishment scheme estimates the trusts of two nodes accurately. In contrast, similar to case 1, the conventional Bayesian method is biased by channel conditions and the relay selection policy and cannot establish an accurate trust value for the relay nodes.

In another experiment, similar to the experiment in Section 6.1, we simulated the situation where the maliciousness probability of a relay node changes at a certain point of the time. Again, starting from the same initial conditions as earlier, we assume that at the 150th iteration, maliciousness of relay node 2 changes to 0.5. The channel conditions are in the high SNR regime. In this experiment, we expect the trust value of relay node 4 to be 0.6 and the

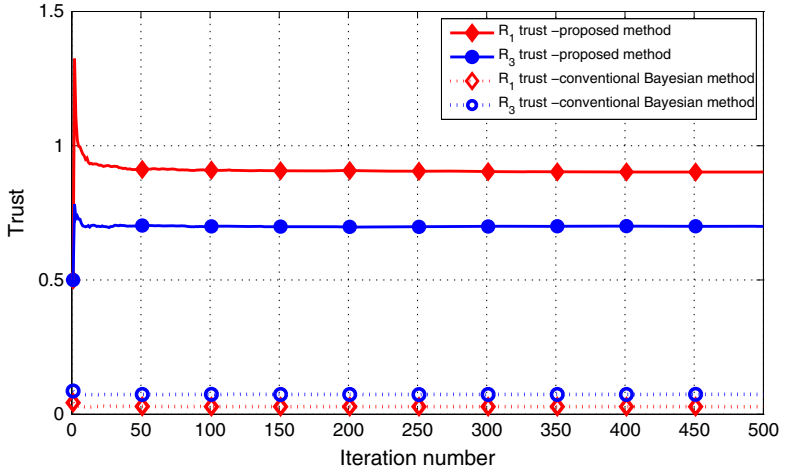



**Figure 8.** Trust establishment in high signal to noise ratio regime in case 2 (with combining).

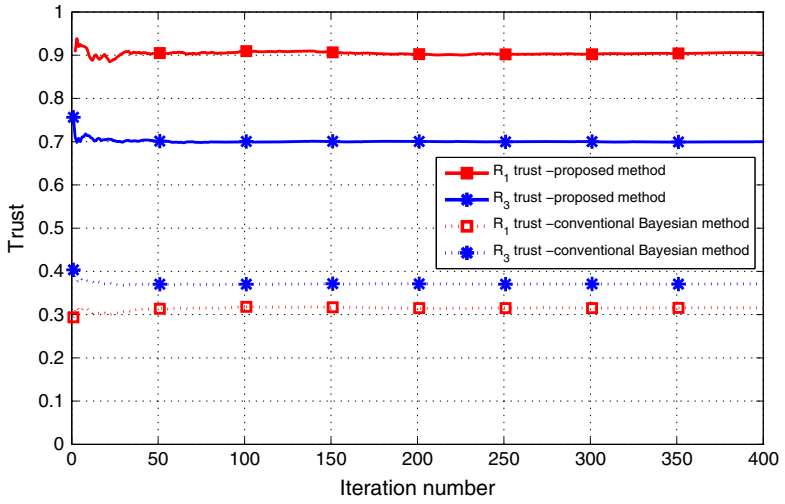



**Figure 9.** Trust establishment in low signal to noise ratio regime in case 2 (with combining).

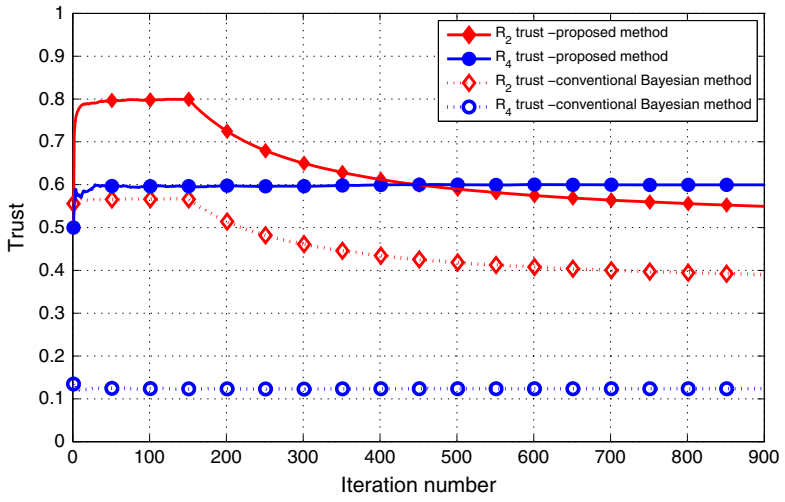



**Figure 10.** Trust tracking with time in case 2 (with combining) in high signal to noise ratio regime.

trust value of relay 2 to change from 0.8 to 0.5 after iteration 150. Therefore, we expect to see the trust value of relay 2 falling below that of relay 4 after iteration 150. As we observe in Figure 10, the conventional Bayesian method gives incorrect trust estimations before and after iteration 150. It also does not satisfy our expectation about the inversion of the rankings of trusts after iteration 150. In contrast, Figure 10 shows that the proposed new method can track the trust accurately. As we see in Figure 10, the response of the trust tracking is not such that it can track rapid changes of trust in the system. To improve the speed of tracking, we use the sliding window approach for the observation process as described earlier in Section 6.1. With a sliding window size of $\omega$, at iteration $t$ and using Equations (22) and (23) when $j = 2$, trust at each iteration $t$ is calculated for the window-based approach. Figure 11 compares the trust for the proposed scheme with and without applying the sliding window of size $\omega = 50$ iterations. Similar to case 1, we observe that trust tracking is much more faster in the case when a sliding window is used.

## 6.3. Multiuser system

In another experiment, the topology shown in Figure 12 was used to observe how the proposed trust establishment works in the presence of malicious relay nodes in a multiuser cooperative network. What makes this experiment distinct from the previous one is that there are four users and three relays for cooperation. Each user has its own channel for its communications. Relays are capable of tuning to the users channel and detecting the users signals simultaneously. In the first phase of a transmission frame, users transmit their signals to all the relays. In the second phase, each relay must be assigned to a user on the basis of the following policy. Those users whose data are received

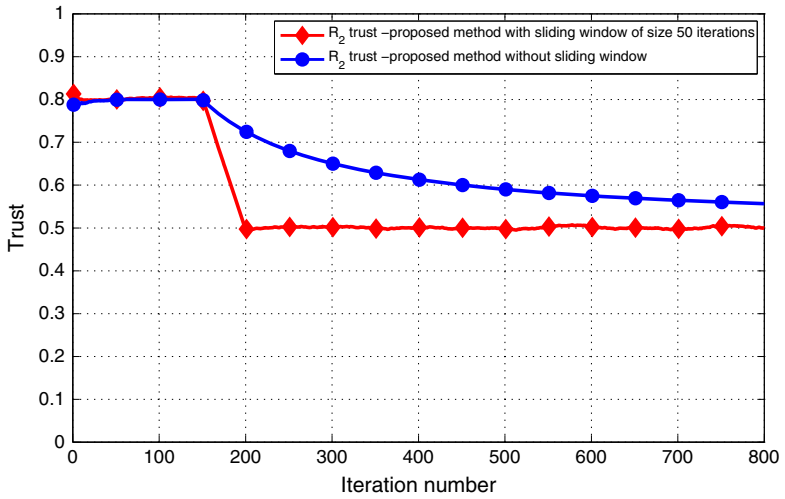



**Figure 11.** Trust tracking with and without using a sliding window in case 2 (with combining) in high signal to noise ratio regime.

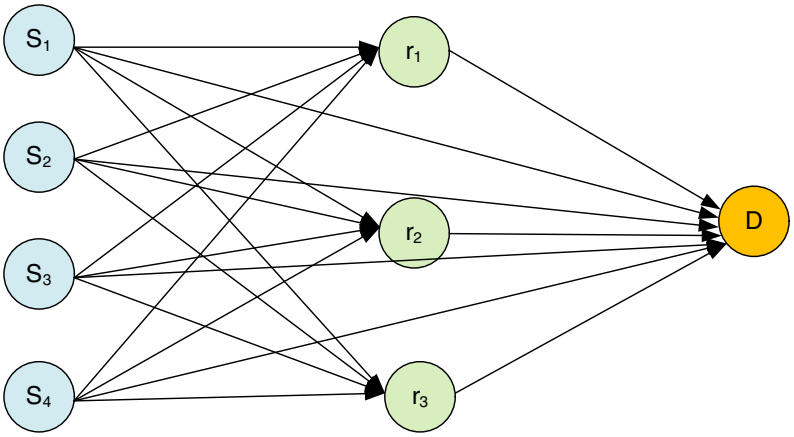



**Figure 12.** Multiuser cooperative relaying system.

correctly at a relay are candidates for assignment to that specific relay. Hungarian algorithm, which is a solution to maximum matching problem, is applied as the policy of relay assignment to the users so that the maximum capacity in the system can be achieved [28,40]. Therefore, the relay selection process is performed according to the solution of the Hungarian algorithm, which is performed by the network controller, that is, node $D$. All the other physical layer parameters of the simulated system are the same as before. The system is working in high SNR regime. Each relay may have a different probability of maliciousness with respect to different users. Maliciousness parameters of relay nodes in the multiuser system are indicated by matrix $q$ as follows.

$$q = \begin{pmatrix} 0.8 & 0 & 0.8 \\ 0.6 & 0 & 0.6 \\ 0.4 & 0 & 0.4 \\ 0.2 & 0 & 0.2 \end{pmatrix}$$

Matrix $q$ is chosen arbitrarily, and similar conclusions can be drawn by using other $q$ matrices. Each element of matrix $q$, that is, $q_{n,i}$, where $n \in \{1,2,3,4\}, i \in \{1,2,3\}$, is in fact $E[Q_{n,i}]$ and denotes the probability of maliciousness of relay $i$ with respect to user $n$. Equivalently, $T_{n,i}$ is trust of relay $i$ with respect to user $n$.

In Figure 13, for clarity of the figure, only four of these trust values are depicted. $T_{1,1}$, the trust value of relay 1 with respect to user 1 is expected to be 0.2 (i.e., $1-E[Q_{1,1}]$). Similarly, we expect $T_{2,3}$, trust value of relay 3 for user 1 to be 0.4, $T_{3,1}$ to be 0.6, and $T_{4,3}$ to be 0.8, respectively. As it is shown in Figure 13, the proposed trust establishment can accurately calculate the trust value of a relay node with respect to a specific user.

### 6.4. Cellular system with mobile users and mobile relays

We also simulated our trust establishment approach in a cellular network with 30 mobile users, 20 mobile relays,

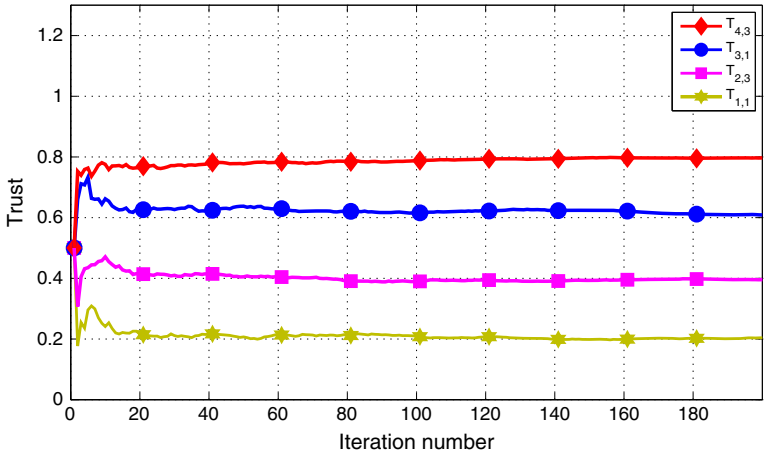



**Figure 13.** Calculated trusts according to the proposed method in multiuser system in high signal to noise ratio regime.

and one base station. The cell over which the users and relays are operating is a 1 Km × 1 Km square shape cell. The system is working in uplink, and the base station acts as the network controller. The base station is located at the center of the cell, and the users and relays are initially distributed uniformly over the cell. The users and relay are mobile, and we used random waypoint model to model the mobility of the nodes over the cell. The power of Rayleigh fading coefficients is distributed exponentially with mean 0.1. The user transmission power is set to 27 dBm, which is equal to the typical transmission power of Global System for Mobile Communications (GSM) handsets. The relay transmission power is set to 30 dBm. The noise power is set to −120 dBm, which is equal to the typical noise power of a 200 KHz GSM channel. We selected a 30 × 20 random matrix $q$ as the matrix of maliciousness probabilities. In other words, each element $q_{n,i}$, where $n \in \{1, 2, \ldots, 30\}, i \in \{1, 2, \ldots, 20\}$, represents the probability of maliciousness of relay $i$ with respect to user $n$. The elements of this matrix are chosen randomly in the interval $[0, 1]$. The applied relay selection policy is the maximum weighted matching policy that was used in the previous simulation [28]. We have run the simulation for 1000 iterations or equivalently $10^5$

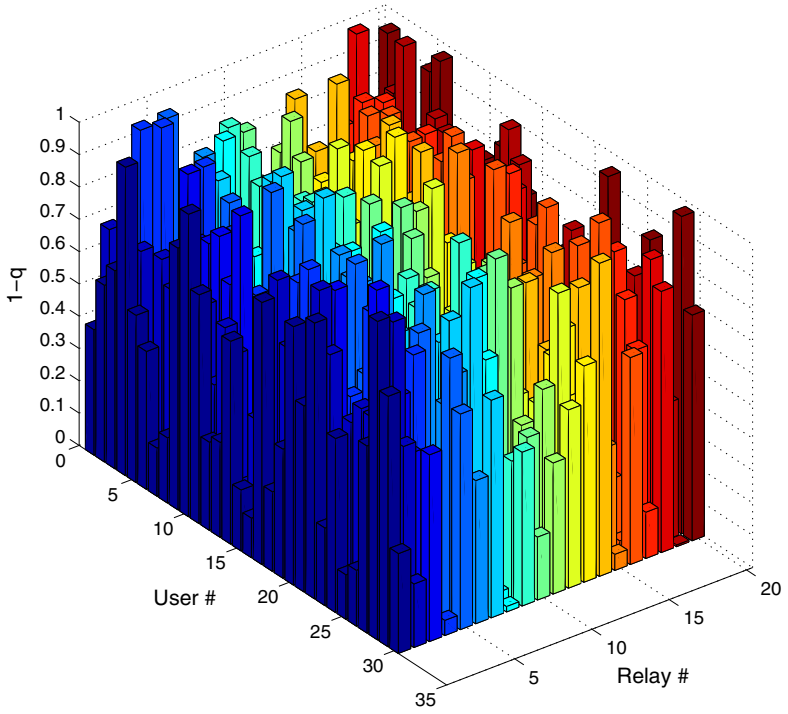



**Figure 14.** Complement of the probabilities of maliciousness.

transmission frames. In this simulation, similar to the previous simulations, we assumed to have two-phase transmission protocol, and we used combining at the base station. We calculated the trust values at each iteration according to Equation (22) with $j = 2$. Figures 14 and 15 depict the complement of maliciousness probabilities and the calculated trust values after iteration 500 (at which point trust values do not have considerable fluctuations)

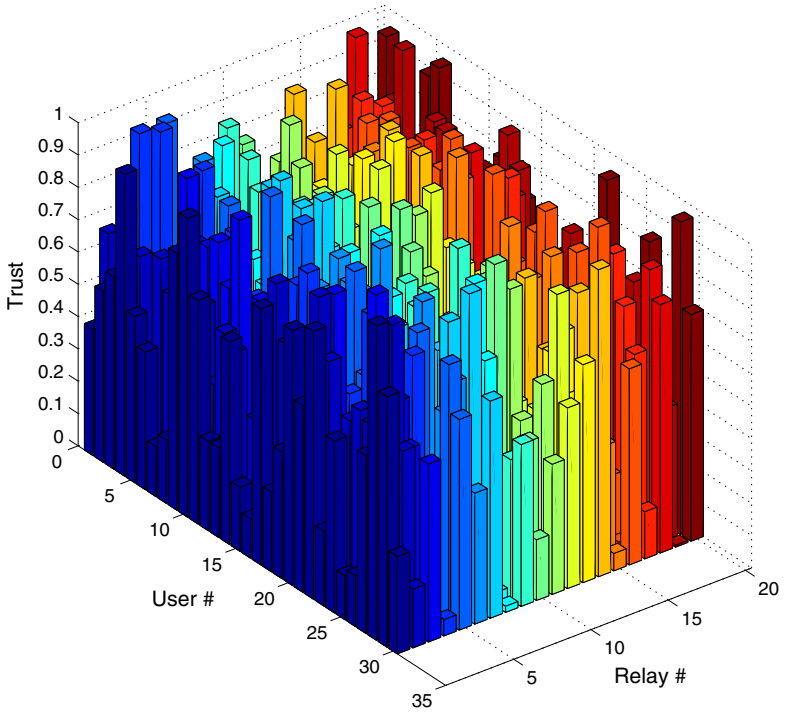



**Figure 15.** Calculated trust values.

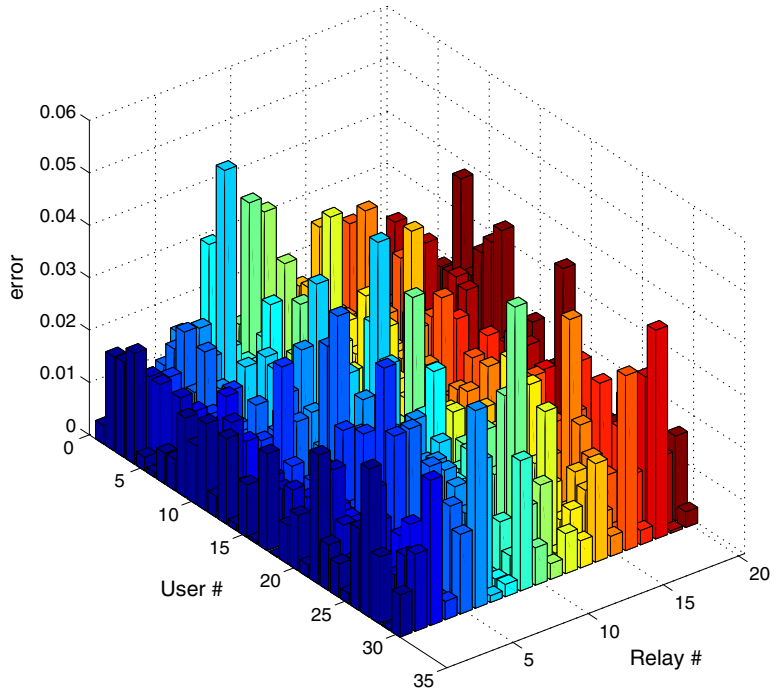



**Figure 16.** Error in calculation of trust values.

in three-dimensional bar plots. As we can see from the figures, all the trust values are between 0 and 1 and are estimating the complement of malicious probabilities nicely. In Figure 16, we calculate the estimation error for each trust value, that is, $|T_{n,i} - \bar{q}_{n,i}|$. It is concluded from the figure that the maximum error in estimating the trust values is less than 0.05. For other trust values, the estimation error is very small (with the average of 0.0111).

## 7. CONCLUSIONS AND FUTURE WORK

In this work, we introduced a trust establishment scheme for cooperative wireless networks. The proposed scheme can be applied to cooperative communication networks with independent channel conditions and relay selection decisions across different transmission frames. We showed that the conventional Bayesian trust establishment method is insufficient to be applied in wireless cooperative networks as it is biased by the channel conditions and relay selection processes. We modified the conventional trust establishment method by incorporating the available information about the channel conditions and relay selection decisions. By using simulations, we demonstrated the effectiveness of the proposed method. In the simulations, we also observed that the speed of trust tracking in case of trust change in the system is relatively low. Therefore, we introduced a sliding window in which we compute the trust values at each iteration on the basis of the observations of just the sliding window (and not all the observations from the beginning). Simulation results confirm the improvement in the speed of trust tracking.

In the proposed method, we always assume that the transmissions, relay selections, or channel conditions are independent across different frames. An interesting problem in this area would be to consider the problem when the aforementioned processes at each frame are history dependent. The simplest case would be to model them as a Markov process. By doing so, a broader class of trust establishment problems in wireless networks could be addressed.

## REFERENCES


1. Sendonaris A, Erkip E, Aazhang B. User cooperation diversity – part I: system description. *IEEE Transactions on Information Theory* 2003; **51**(11): 1927–1938.
2. Kramer G, Gastpar M, Gupta P. Cooperative strategies and capacity theorems for relay networks. *IEEE Transactions on Information Theory* 2005; **51**(9): 3037–3063.
3. Laneman N, Tse D, Wornell G. Cooperative diversity in wireless networks: efficient protocols and outage behavior. *IEEE Transactions on Information Theory* 2004; **50**(12): 3062–3080.
4. Kramer G, Maric I, Yates RD. *Cooperative Communications*. Foundations and Trends in Networking, NOW Publishers: Hanover MA, 2007.
5. Liu J, Yu FR, Lung CH, Tang H. Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks. *IEEE Transactions on Wireless Communications* 2009; **8**(2): 806–815.
6. Yu FR, Tang H. Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks. *Wireless Networks* 2010; **16**(8): 2169–2178.
7. Bu S, Yu FR, Liu P, Mason P, Tang H. Distributed combined authentication and intrusion detection with data fusion in high security mobile ad-hoc networks. *IEEE Transactions on Vehicular Technology* 2011; **60**(3): 1025–1036.
8. Mao Y, Wu M. Tracing malicious relays in cooperative wireless communications. *IEEE Transactions on Information Forensics and Security* 2007; **2**(2): 198–212.
9. Mao Y, Wu M. Security issues in cooperative communications: tracing adversarial relays, In *Proceedings of the IEEE International Conference on Acoustic, Speech, and Signal Processing. ICASSP'06*, Toulouse, France, 2006; IV 69–IV 72.
10. Changiz R, Halabian H, Yu FR, Lambadaris I, Tang H. Trust management in wireless mobile networks with cooperative communications, In *Proceedings of the IEEE/IFIP TrustCom 2010*, HongKong, P.R. China, 2010; 498–503.
11. Changiz R, Halabian H, Yu FR, Lambadaris I, Tang H, Mason PC. Trust establishment in cooperative wireless networks, In *IEEE Milcom 2010*, San Jose, CA, USA, 2010; 1074–1079.
12. Zouridaki C, Mark BL, Hejmo M, Thomas RK. A quantitative trust establishment framework for reliable data packet delivery in manets, In *Proceedings of 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'05))*, Alexandria, USA, 2005; 1–10.
13. Dehnie S, Sencar HT, Memon N. Detecting malicious behavior in cooperative diversity, In *Proceedings of Conference on Information Sciences and Systems. CISS'07*, Baltimore, USA, 2007; 895–899.
14. Dong L, Han Z, Petropulu A, Poor H. Improving wireless physical layer security via cooperating relays. *IEEE Transactions on Signal Processing* 2010; **58**(3): 1875–1888.
15. Buchegger S, Boudec JYL. A robust reputation system for P2P and mobile ad-hoc networks, In *Proceedings of 2nd Workshop on Economics of Peer-to-Peer Systems*, Boston, MA, 2004; 1–6.

16. Jiang X, Lin C, Yin H, Chen Z, Su L. Game-based trust establishment for mobile ad hoc networks, In *Proceedings of 2009 WRI International Conference on Communications and Mobile Computing (CMC'09)*, Kunming, Yunnan, China, 2009; 475–479.
17. Shankaran R, Varadharajan V, Orgun MA, Hitchens M. Context-aware trust management for peer-to-peer mobile ad-hoc networks, In *Proceedings of 33rd IEEE Computer Software and Applications Conference (COMPSAC'09)*, Seattle, WA, 2009; 188–193.
18. Chang BJ, Kuo SL. Markov chain trust model for trust-value analysis and key management in distributed multicast manets. *IEEE Transactions on Vehicular Technology* 2009; **58**(4): 1846–1863.
19. Quercia D, Hailes S, Capra L. B-trust: Bayesian trust framework for pervasive computing, In *Proceeding of 4th International Conference on Trust Management*, Pisa, Italy, 2006; 298–312.
20. Proakis JG. *Digital Communications*, (4th edn). McGraw-Hill: New York, NY, 2001.
21. He X, Yener A. Two-hop secure communication using an untrusted relay: a case for cooperative jamming, In *Proceedings of the IEEE Global Telecommunications Conference. GLOBECOM'08*, New Orleans, USA, 2008; 1–5.
22. Perron E, Diggavi S, Telatar E. On cooperative wireless network secrecy, In *Proceedings of the IEEE Infocom 2009*, Rio de Janiero, Brazil, 2009; 1935–1943.
23. Davison AC. *Statistical Models*. Cambridge University Press: London, 2003.
24. Berger J. *Statistical Decision Theory and Bayesian Analysis*. Springer-Verlag: London, 1985.
25. Wang B, Han Z, Liu KJR. Distributed relay selection and power control for multiuser cooperative communication networks using stackelberg game. *IEEE Transactions on Mobile Computing* 2009; **8**: 975–990.
26. Onat FA, Fan Y, Yanikomeroglu H, Poor HV. Threshold based relay selection in cooperative wireless networks, In *Proceedings of the IEEE Globecom 2008*, New Orleans, LA, 2008; 1–5.
27. Sreng V, Yanikomeroglu H, Falconer DD. Relayer selection strategies in cellular networks with peer-to-peer relaying, In *Proceedings of the IEEE VTC'F03*, Orlando, FL, 2003; 1949–1953.
28. Halabian H, Lambadaris I, Lung CH, Srinivasan A. Throughput-optimal relay selection in multiuser cooperative relaying networks, In *IEEE MILCOM 2010*, San Jose, CA, USA, 2010; 507–512.
29. Dehnie S, Memon N. A stochastic model for misbehaving relays in cooperative diversity, In *Proceedings of the IEEE WCNC 2008*, Las vegas, USA, 2008; 482–487.
30. Capra L. Toward a human trust model for mobile ad-hoc networks, In *Proceedings of 2nd UK-UbiNet Workshop*, Cambridge, UK, 2004; 1–2.
31. Cho JH, Swami A, Chen IR. A survey on trust management for mobile ad hoc networks. *IEEE Communications Surveys and Tutorials* 2011; **13**(4): 562–583.
32. Heer T, Götz S, Morchon OG, Wehrle K. ALPHA: an adaptive and lightweight protocol for hop-by-hop authentication, In *Proceedings of the ACM CoNEXT Conference*, Madrid, Spain, 2008; 1–12.
33. Ramamoorthy R, Yu FR, Tang H, Mason P, Boukerche A. Joint authentication and quality of service provisioning in cooperative communication networks. *Computer Communications* 2012; **35**(5): 597–607.
34. Merkle RC. A certified digital signature, 1979.
35. Makda S, Choudhary A, Raman N, Korakis T, Tao Z, Panwar S. Security implications of cooperative communications in wireless networks, In *Proceedings of the IEEE Sarnoff Symposium*, Princeton, USA, 2008; 1–6.
36. Beres E, Adve R. Selection cooperation in multi-source cooperative networks. *IEEE Transactions on Wireless Communications* 2008; **7**(1): 118–127.
37. Ng TCY, Yu W. Joint optimization of relay strategies and resource allocations in cooperative cellular networks. *IEEE Journal on Selected Areas in Communications* 2007; **25**(2): 328–339.
38. Ibrahim A, Sadek AK, Su W, Liu KJR. Cooperative communications with relay selection: when to cooperate and whom to cooperate with? *IEEE Transactions on Wireless Communications* 2008; **7**: 2814–2827.
39. Wei Y, Yu FR, Song M. Distributed optimal relay selection in wireless cooperative networks with finite-state markov channels. *IEEE Transactions on Vehicular Technology* 2010; **59**(5): 2149–2158.
40. Kuhn HW. The hungarian method for the assignment problem. *Naval Research Logistic Quarterly* 1955; **2**: 83–97.

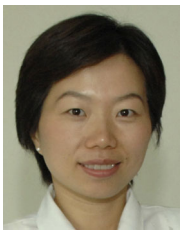
## AUTHORS' BIOGRAPHIES

**Reyhaneh Changiz** was born in Isfahan, Iran, in 1984. She received her BSc degree in Electrical Engineering from Isfahan University of Technology, Isfahan, Iran in 2007. In September 2009, she joined BroadBand Networks Laboratory, Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, where she is currently pursuing her MASc degree. Her research interests include digital communication and wireless cooperative communication.

**Hassan Halabian** was born in Isfahan, Iran, in 1983. He received his BSc and MASc degrees in Electrical Engineering from Isfahan University of Technology, Isfahan, Iran in 2005 and 2008, respectively. In September 2008, he joined BroadBand Networks Laboratory, Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada, where he is currently pursuing his PhD degree. His research interests include stochastic network optimization for wireless networks, queueing systems, and information theory.

**F. Richard Yu** (S'00-M'04-SM'08) received his PhD degree in Electrical Engineering from the University of British Columbia (UBC) in 2003. From 2002 to 2004, he was with Ericsson (in Lund, Sweden), where he worked on the research and development of 3G cellular networks. From 2005 to 2006, he was with a start-up in California, U.S.A., where he worked on the research and development in the areas of advanced wireless communication technologies and new standards. He joined Carleton School of Information Technology and the Department of Systems and Computer Engineering at Carleton University in 2007, where he is currently an associate professor. He received the Carleton Research Achievement Award in 2012, Ontario Early Researcher Award in 2011, Excellent Contribution Award at IEEE/IFIP TrustCom 2010, Leadership Opportunity Fund Award from Canada Foundation of Innovation in 2009, and Best Paper Awards at IEEE/IFIP TrustCom 2009 and Int'l Conference on Networking 2005. His research interests include cross-layer design, security, and QoS provisioning in wireless networks. He is a senior member of the IEEE. He serves on the editorial boards of several journals, including IEEE Transactions on Vehicular Technology, IEEE Communications Surveys & Tutorials, ACM/Springer Wireless Networks, EURASIP Journal on Wireless Communications Networking, Ad Hoc & Sensor Wireless Networks, Wiley Journal on Security and Communication Networks, and International Journal of Wireless Communications and Networking. He has served on the Technical Program Committee (TPC) of numerous conferences, as the TPC co-chair of IEEE INFOCOM-GCN'2012, ICC-GCN'2012, VTC'2012S, Globecom'11, INFOCOM-GCN'2011, INFOCOM-CWCN'2010, IEEE IWCMC'2009, VTC'2008F, and WiN-ITS'2007, as the publication chair of ICST QShine 2010, and the co-chair of ICUMT-CWCN'2009.

**Ioannis Lambadaris** (M'02) was born in Thessaloniki, Greece. He received his Diploma degree in Electrical Engineering from the Polytechnic School, Aristotle University of Thessaloniki, Thessaloniki, Greece, in 1984, MSc degree in Engineering from Brown University, Providence, RI, in 1985, and PhD degree in Electrical Engineering from the Department of Electrical Engineering, Systems Research Center (SRC), Institute for Systems Research (ISR), University of Maryland, College Park, in 1991. After finishing his graduate education, he was a research associate at Concordia University, Montreal, QC, Canada, from 1991 to 1992. From September 1992, he was with the Department of Systems and Computer Engineering, Carleton University, Ottawa, ON, Canada. Currently, he is a professor in the same department. His interests lie in the area of applied stochastic processes and their application for modeling and performance analysis of computer communication networks and wireless networks. His current research concentrates on quality-of-service (QoS) control for IP and evolving optical networks architectures and stochastic control/optimization in emerging wireless networks. His research is carried out in close collaboration with his students and colleagues in the Broadband Networks Laboratory (http://www.sce.carleton.ca/bbnlab/bnlhome.shtml). He received a Fellowship from the National Fellowship Foundation of Greece (1980–1984) during his undergraduate studies. He also received the Technical Chamber of Greece Award (ranked first in graduating class). He was a recipient of a Fulbright Fellowship (1984–1985) for graduate studies in the U.S., whereas at Carleton University, he received the Premiers Research Excellence Award, and the Carleton University Research Excellence Award (2000–2001), for his research achievements in the area of modeling and performance analysis of computer networks.



**Helen Tang** received her PhD degree in the Department of Systems and Computer Engineering from Carleton University in 2005. From 1999 to 2005, she had worked in a few R&D organizations in Canada and USA including Alcatel-Lucent, Mentor Graphics, and Communications Research Center Canada. In October 2005, she joined Network Information Operations Section at Defence R&D Canada as a defence scientist. She is a member of IEEE. She has published more than 20 research papers in international journals and conferences including IEEE Transactions on Wireless Communications, Journal of Security and Comm. Networks, IEEE ICC, IEEE VTC, IEEE Milcom, and IEEE Globecom. She has served as reviewer, session chair, and technical committee member for various conferences. Her research interests include ad hoc and sensor networks, wireless network security, communication protocols, and performance analysis.


*Wirel. Commun. Mob. Comput.* 2014; **14**:1450–1470 © 2012 John Wiley & Sons, Ltd.
DOI: 10.1002/wcm