An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Dropping Attack in Multihop Wireless Networks

Mohamed Elsalih Mahmoud and Xuemin (Sherman) Shen, *Fellow, IEEE*

***Abstract*—In multihop wireless networks, the rational packet droppers may not relay others' packets because packet relay consumes their resources without benefits and the irrational packet droppers drop packets intentionally to disrupt the packet-transmission process, which may fail the multihop communication. Cooperation stimulation mechanisms can motivate the rational packet droppers to relay packets, but they cannot identify the irrational packet droppers. In this paper, we develop a mechanism called TRIPO that adopts stimulation and punishment strategies for thwarting packet dropping attack. TRIPO uses micropayment to stimulate the rational packet droppers to relay others' packets and enforce fairness, and uses reputation system to identify and evict the irrational packet droppers. We propose a novel monitoring technique to measure the nodes' frequency of dropping packets based on processing the payment receipts instead of using medium overhearing technique. The receipts can be processed to extract financial information to reward the cooperative nodes that relay packets, and contextual information, such as the broken links, to build up the reputation system. Extensive analytical and simulation results demonstrate that TRIPO can secure the payment and precisely identify the irrational packet droppers with almost no false-positive nodes, which can improve the network performance in terms of packet-delivery ratio.**

***Index Terms*—*Cooperation stimulation, reputation systems, gray/black hole attacks, and packet-dropping attack.*

1. Introduction

MULTIHOP wireless networks (MWNs) have been emerging for enabling new applications and enhancing the network performance and deployment [1], [2], [3]. In MWNs, the mobile nodes act as routers to relay the source nodes' packets to their destinations. Multihop packet relay can extend the communication range using limited transmit power and enhance the network throughput and capacity [4], [5]. Moreover, MWNs can be deployed more readily and at low cost in developing and rural areas. However, the reliability of the packet-relaying nodes cannot be guaranteed because they are autonomous and self-interested, which endangers the network proper operation.

The rational packet droppers do not cooperate in relaying packets because packet relay consumes their valuable resources, such as energy and computing power, without any immediate benefits. Moreover, the irrational packet droppers, such as compromised and faulty nodes, involve themselves in communication sessions with the intention of dropping the packets to disrupt the packet-transmission process. Note that the words "route" and "session" are used exchangeably in this paper. *Packet-Dropping* attack considerably degrades the network connectivity and performance in terms of packet delivery ratio and throughput and the presence of even a small number of attackers results in repeatedly dropped packets, which may fail the multihop communication [7], [8].

Cooperation stimulation mechanisms [9], [10] use credits (or micropayment) to motivate the rational packet droppers to relay packets. The nodes earn credits for relaying others' packets and spend them to relay their packets, i.e., these mechanisms make relaying packets more beneficial for the nodes than dropping them. However, cooperation stimulation mechanisms cannot identify the irrational packet droppers assuming that the nodes will relay the packets faithfully with using credits. This assumption cannot be guaranteed in MWNs because, unlike single-hop networks that are run by the equipments of the operators, packet-relay is performed by user provided equipment. Some attackers may drop packets to disrupt the packet-transmission process and broken nodes may have a software or hardware fault that prevents them from relaying the packets successfully. In IP networks, the malfunction of the network equipments is an important source for the network unavailability [11]. It is impossible to know whether a packet is dropped for malicious or non-malicious reasons, e.g., due to faulty nodes and bad channel condition, so it is necessary to measure the nodes' frequency of dropping packets and the nodes that consistently drop the packets are considered attackers because they pose a severe threat to the network proper operation [9], [10].

In this paper, we develop **TRIPO**, a novel mechanism that can **T**hwart the **R**ational and **I**rrational **P**acket dropping attacks by adopting stimulation and punishment strategies. TRIPO uses credits to stimulate the rational packet droppers to relay packets, and uses reputation system to identify and evict the irrational packet droppers. With TRIPO, uncooperation will not be an abuse because the nodes are stimulated and not forced to relay others' packets using their own devices because packet relay incurs a cost of energy and other resources, but frequently dropping packets are an obvious abuse due to disrupting the network proper operation. Since a trusted party may not be involved in a communication route, the nodes in the route submit receipts (proofs of packet-relay) to an offline trusted party. For efficient implementation, we propose a novel tech-

Manuscript received April 14, 2011; revised June 13, 2011; accepted July 20, 2011. First published ****; current version published **. The review of this paper was coordinated by Dr. Phone Lin.

M. Mahmoud and X. Shen are with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: mmabdels@bbcr.uwaterloo.ca; xshen@bbcr.uwaterloo.ca).

A part of this paper was presented at IEEE GLOBECOM'10 conference [6].

nique for measuring the nodes' frequency of dropping packets based on processing the receipts instead of using the traditional medium overhearing technique [9], [10]. The trusted party can process the receipts to extract financial information to reward the intermediate nodes and charge the source and destination nodes, and contextual information, such as the broken link, to build up a reputation system to identify the irrational packet droppers. A node's reputation value is degraded whenever it is involved in a broken link, otherwise it is improved. A node is identified as irrational packet dropper and excluded from the network when its reputation value degrades to a threshold because it becomes a threat to the network proper operation and its packet dropping action is genuine and cannot be temporary. Securing the route discovery is outside the scope of this work that focuses on thwarting *Packet-Dropping* attacks, but TRIPO can be implemented on the top of a secure routing protocol such as [12] and [13].

In addition to thwarting *Packet-Dropping* attack, TRIPO can enforce fairness, discourage *Resource-Exhaustion* attack, and efficiently charge the future services. The fairness issue arises when some nodes take advantage of the network more than others. For example, although the nodes situated at the network center relay more packets than others, they are not compensated. Moreover, the nodes that use the network more generate more traffic than others. In order to enforce fairness, TRIPO can compensate the nodes that relay more packets by rewarding credits. Since the nodes pay for relaying their packets, TRIPO can discourage launching *Resource-Exhaustion* attack by sending spurious packets to exhaust the resources of the intermediate nodes. TRIPO can also be used for charging the future services of the wireless networks because the communication sessions may occur without involving an infrastructure and the mobile nodes may roam among different foreign networks [14], [15]. Extensive analytical and simulation results demonstrate that TRIPO can secure the payment and precisely identify and evict the irrational packet droppers with almost no false-positive nodes, which can improve the network connectivity and performance in terms of packet delivery ratio and throughput.

The main contributions of this paper are four-fold: (1) This is the first work that points out that cooperation stimulation alone is not sufficient for thwarting *Packet-Dropping* attack, and TRIPO is the first mechanism that adopts stimulation and punishment strategies for thwarting *Packet-Dropping* attack in MWNs; (2) We propose a novel technique for monitoring the nodes' frequency of dropping packets based on processing the payment receipts instead of using medium overhearing technique; (3) We develop a novel reputation system that can precisely identify the irrational packet droppers; and (4) We program a simulator to evaluate TRIPO and the simulation results demonstrate that all the irrational packet droppers can be identified with almost no false-positive nodes.

The remainder of this paper is organized as follows. Section 2 reviews the related works. Section 3 presents the system models and Section 4 proposes TRIPO. Security analysis and performance evaluation are given in Sections 5 and 6, respectively, followed by conclusion and future work in Section 7.

2. Related Works

For cooperation stimulation mechanisms, the intermediate nodes usually compose undeniable proofs of relaying the packets, called payment receipts, which contain the identities of the payers and the payees and the payment amount. Since the connection to a trusted centralized unit, called the accounting center (AC), may not be available on regular basis, the nodes accumulate the receipts and submit then when the connection is possible to update their credit accounts. For cooperation enforcement mechanisms, each node usually monitors the transmissions of its neighbors to make sure that the neighbors relay others' packets, and thus packet droppers (rational or irrational) can be identified and punished.

2.1 Cooperation Stimulation Mechanisms

In Sprite [16], the source node signs the identities of the nodes in the route and appends the signature to its message. The intermediate nodes verify the signature and compose signed receipts. Using game theory, Sprite determines the charges and rewards to motivate each node to report its message forwarding activities honestly and proves the correctness of the proposed mechanism. Ad hoc-VCG [17] uses game theory for routing the packets through greedy and selfish nodes that accept payments for forwarding others' packets if the payments cover the costs, such as energy, incurred in forwarding the packets. They have shown that it is in the nodes' best interest to reveal their true costs for forwarding messages and the mechanism guarantees that routing is done along the most cost efficient path in a game-theoretic sense by paying to the intermediate nodes a premium over their actual costs of forwarding packets.

Unlike Sprite that charges only the source node no matter how the destination node is interested in the communication, FESCIM [18] adopts fair charging policy by charging both the source and destination nodes when both of them are interested in the communication. In PIS [19], the source node attaches a signature to each message and the destination node replies with a signed *ACK*. PIS can reduce the receipts' number by generating a fixed-size receipt per session regardless of the number of messages instead of generating a receipt per message in Sprite. ESIP [20] proposes a communication protocol that can be used for a cooperation stimulation mechanism. The protocol uses the public key cryptography and the identity based cryptography to reduce the number of signing and verifying operations. The source and destination nodes generate hash chains and sign their roots. For each message, the source node appends the pre-image of the last sent hash value from its chain and a keyed hash value for each intermediate node to ensure the message integrity at each hop. The destination node replies with *ACK* packet containing the pre-image of the last sent hash value from its chain. By this way only two signatures can be generated for the whole session, i.e., one signature from the source node and one signature from the destination node. In [21], instead of submitting payment receipts to the AC, each node submits a brief payment report containing its alleged charges and rewards of different sessions. The AC uses lightweight statistical methods to identify the cheating nodes that report

incorrect payment. However, due to the nature of the statistical methods, the colluding nodes may manage to steal credits and the payment clearance may be long delayed until identifying the cheating nodes that submit incorrect reports.

Different from these works, TRIPO can identify the irrational packet droppers. Although the proposed protocol in ESIP can be used with TRIPO, we use simple communication protocol due to space limitation and to focus on our contribution, i.e., identifying the irrational packet droppers.

2.2 Cooperation Enforcement Mechanisms

In [7], two modules called watchdog and path-rater are implemented in each node. When node A transmits a packet to B to relay to C, the watchdog module of node A overhears the medium to make sure that B relays the packet. Node A increases the reputation value of node B when it overhears the packet relay; otherwise, node A decreases the reputation value of B. Node A accuses B of dropping packets as soon as its reputation value degrades to a threshold. Based on the watchdog's accusations, the path-rater module chooses the path that avoids the packet droppers without punishing them, which imposes extra load on the honest nodes without compensation. In OCEAN [22], a node's reputation value is initialized to neutral (0), every positive behavior (relaying a packet) results in an increment (+1), and every negative behavior (dropping a packet) results in a decrement (−2). Once a node's reputation value falls below a threshold (−40), the node is identified as packet dropper. However, in [7] and [22], the nodes depend only on their observations to evaluate the packet dropping frequency of the other nodes and they do not share their evaluations, which may degrade the effectiveness of the mechanism because the honest nodes that drop the packets temporarily, e.g., due to the network congestion or other reasons, may be falsely identified as packet droppers.

For CONFIDANT [23] and CORE [24], each node combines its evaluation with the evaluations of other nodes to calculate a node's reputation value. Only the positive evaluations are propagated in CORE to prevent maliciously defaming the nodes' reputations by propagating negative evaluations, and only the negative evaluations are propagated in CONFIDANT to prevent the colluding nodes from falsely boosting their reputations by propagating positive evaluations. However, in order to precisely judge the real behavior of a node, both the negative and positive behaviors should be considered. Moreover, in CORE and CONFIDANT, the packet droppers are isolated from the network unilaterally by each node by avoiding them in routing and denying relaying their packets, which may result in widespread false accusations because when node A denies relaying the packets of a packet dropper, the neighbors of A may consider its behavior illegal.

In SORI [25], each node counts the number of packets relayed both by and for a neighboring node, and the ratio of these counts is combined with reports from other nodes to calculate the node's reputation value. However, the less frequently selected nodes by the routing protocol such as those at the network perimeter have bad reputation falsely. In [26], 2-hop *ACK* technique is used to monitor the nodes' frequency of dropping packets instead of using the medium overhearing technique. Node A accuses the neighboring node B of dropping a packet if node A does not receive *ACK* from the 2-hop away node C, but the mechanism completely fails when two neighboring nodes collude to issue fake *ACK*s.

TABLE 1: COMPARISON BETWEEN COOPERATION ENFORCEMENT MECHANISMS AND TRIPO.

	Cooperation enforcement mechanisms	**TRIPO**
Monitoring technique	Overhearing the medium channel.	Processing the payment receipts.
Fairness	The nodes that relay more packets are not compensated.	Credits are used to compensate the nodes that relay more packets.
Motivations	Relaying others' packets and running the monitoring technique consume the nodes' resources without direct benefits.	Relaying others' packets and submitting the receipts are beneficial for the nodes for earning credits.
Effectiveness	- The nodes' mobility may not allow precisely assessing their behavior. - Inaccuracy due to packet collision. - The attackers can adjust the transmission power to circumvent the mechanism.	The TP can monitor the nodes over a long time and different sessions to precisely judge their behaviors.

The main differences between the cooperation enforcement mechanisms and TRIPO are given in Table 1. The cooperation enforcement mechanisms cannot enforce fairness because they do not compensate the nodes that relay more packets such as those situated at the network center and force the nodes to relay others' packets without any benefits and punish them when they do not cooperate no matter how they have previously contributed to the network. In cooperation enforcement mechanisms, misbehavior is beneficial for the nodes, e.g., the nodes may relay the packets to avoid punishment, but they do not monitor their neighbors to save their resources and make use of the other nodes' evaluations to avoid routing their packets through the packet droppers, which degrades the effectiveness of the mechanisms. Moreover, to differentiate between a node's unwillingness and incapability to relay packets, the cooperation enforcement mechanism should monitor the nodes over long time and different sessions because packet drop may just happen accidently, e.g., due to low resources, node mobility, bad channel condition, and network congestion, but the mechanisms may not have sufficient time to precisely judge a node's behavior due to the node mobility.

In addition, the medium overhearing technique suffers from inefficiency and inaccuracy problems because the assumption that the transmitted packets by a node can be overheard by all the nodes in its neighborhood cannot be ensured for the following reasons: (1) When node B relays a packet to C, node A cannot overhear the packet relay because of packet collision, i.e., due to another concurrent transmission in its neighborhood [27]; (2) Since node A can know if B has relayed a packet but cannot know if C received it, node B can save its power and circumvent the monitoring technique if node A is closer than node C by adjusting its transmission power such that the signal is strong enough to be overheard by the monitoring node A but too weak to be received by the true recipient node C [27]; and

(3) The overhearing monitoring technique is not power efficient for transmitters because they have to use the full transmission power instead of adapting the power according to the distance separating the transmitter and the receiver to avoid false accusations [28]. For example, if the required power to relay packets from B to C is less than the required power to reach A from B, the packets sent from B to C will not be overheard by A. Consequently, node A will not be able to validate any packet relay event by node B and thus may wrongly accuse B of dropping the packets.

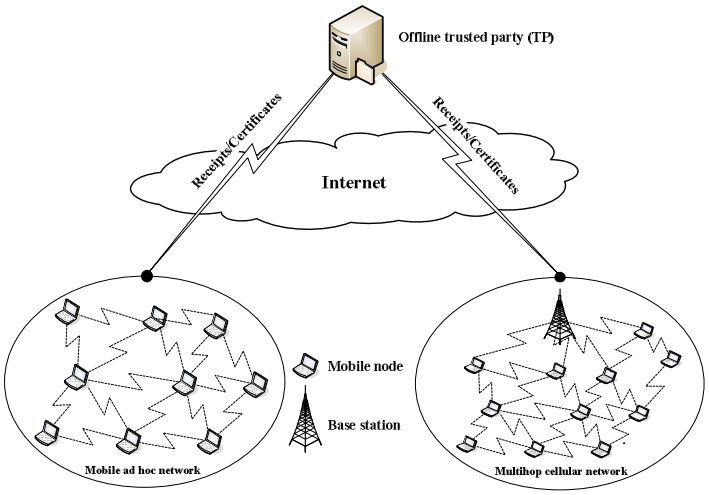


Fig. 1: The architecture of multihop wireless networks.

3. System Models

3.1 Network and Communication Models

As illustrated in Fig. 1, the considered multihop wireless network includes an offline trusted party (TP), mobile nodes, and base stations in some networks. The TP contains the accounting center (AC) and the reputation system (RS). The TP generates private/public key pair and certificate with unique identity for each node to participate in the network. Once the TP receives the payment receipts from the network nodes, it processes them to extract financial and contextual information. The financial information is passed to the AC to update the nodes' credit accounts, and the contextual information is passed to the RS to update the nodes' reputation values. Once the RS detects an irrational packet dropper, the TP revokes the node by not renewing its certificate. TRIPO can be implemented on the top of any on-demand routing protocol, such as DSR [29], to establish an end-to-end route between the source and the destination nodes. The source node's packets may be relayed several hops by the intermediate nodes to the destination node. The nodes can contact the TP at least once during a period, called updating time, which can be in the range of few days. During this connection, the nodes submit the receipts and renew their certificates. This connection can occur via the base stations, Wi-Fi hotspots, or wired networks such as Internet.

3.2 Threat and Trust Models

The mobile nodes and the base stations are probable attackers but the TP is fully secure. The mobile nodes are autonomous and self-interested and the base stations may belong to different operators that are motivated to misbehave, e.g., to steal credits. It is impossible to realize secure payment between two entities without a trusted third party [30]. The attackers can be classified into two classes: rational attackers and irrational packet droppers. The rational attackers misbehave when they can achieve more benefits than behaving honestly. Specifically, they attempt to steal credits, pay less, and communicate freely. On the contrary, the irrational packet droppers aim to disrupt the packet-transmission process by dropping the packets without considering their interests and the attack cost such as energy and credits. The irrational packet droppers may launch *Black-Hole* attack by continuously dropping all the packets they are supposed to relay, or *Gray-Hole* attack by intentionally dropping the packets in some sessions and behaving regularly in other sessions to circumvent the reputation system but the ratio of misbehaving sessions should be large to launch effective attacks. The irrational packet droppers may be compromised, malfunctioned, or faulty nodes.

The attackers have full control on their nodes and thus they can change the nodes' operation. Uncooperation in relaying others' packets will not be an abuse because the nodes are stimulated and not forced to relay others' packets using their own devices, but the high frequency of dropping packets is an abuse due to disrupting the network proper operation. The attackers may work individually or collude with each other to launch sophisticated attacks. The colluding irrational packet droppers may launch *Reputation-Boost* and *False-Accusation* attacks.
For the *Reputation-Boost* attack, the attackers attempt to falsely augment their reputations to escape the consequence of dropping the packets; and for the *False-Accusation* attacks, the attackers attempt to defame the reputation values of some honest nodes to evict them from the network. The gained experience from the currently used mechanisms and protocols in civilian applications emphasizes that the large-scale irrational collusion attacks are highly unlikely [31], [32]. The reputation systems are susceptible to collusion attacks due to the nature of these systems. Our objective is to protect the payment against the large-scale collusion attacks and protect the reputation system against the small-scale irrational collusion attacks launched by a low number of colluders, e.g., in the range of ten, and improve the robustness of the reputation system against the large-scale collusion attacks.

For the trust models, the network nodes fully trust the TP to manage their credit accounts and reputation values, but the TP does not trust any node in the network.

3.3 Payment Model

We adopt fair and general-purpose charging policy by supporting cost sharing between the source and the destination nodes when both of them are interested in the communication. The payment-splitting ratio is service-dependent and depends on the beneficiary of the communication, e.g., the ratio is 0.5 if the source and destination nodes are equally interested in the communication and DNS server should not pay for name resolution. For the rewarding policy, TRIPO can be integrated with any rewarding policy such as the proposed one in [17] that

considers that the reward for relaying a packet is proportional to the incurred energy in relaying the packet. However, to focus on our contributions, similar to [18], [19], [20], [21], we use fixed rewarding rate, e.g., λ credits per unit-sized packet. The AC charges the source and the destination nodes for every transmitted message even if it does not reach to the destination node, but the AC rewards the intermediate nodes only for the delivered messages. Table 2 gives the used notations in this paper.

TABLE 2: THE USEFUL NOTATIONS.

Symbol	Description
X, Y	X is concatenated to Y.
CSR(X)	Complete session receipt for *X* delivered messages.
H(M)	The hash value resulted from hashing M.
ID_A	The identity of an intermediate node A.
ID_S and ID_D	The identities of the source node (S) and the destination node (D), respectively.
ISR(X)	Incomplete session receipt for *X*-1 delivered messages and one sent message.
M_X	The message sent in the *X*th data packet.
$R_{St,A}(t)$ and $R_{Lt,A}(t)$	The short-term and the long-term reputation values of node A at time t, respectively, where $R_{St,A}(t)$ and $R_{Lt,A}(t) \in [0, 1]$.
$S_A(t)$	The state of node A at time t. $S_A(t) \in \{+1, 0, -1\}$ which corresponds to {Honest, Suspicious, Evicted}.
SI	The session identifier that includes the identities of the nodes in the session and the time stamp of the session establishment (TS).
$Sig_A(X)$	The signature of an intermediate node A on X.
$Sig_S(X)$ and $Sig_D(X)$	The signatures of the source and the destination nodes on X, respectively.
TS	The time stamp of a session establishment.

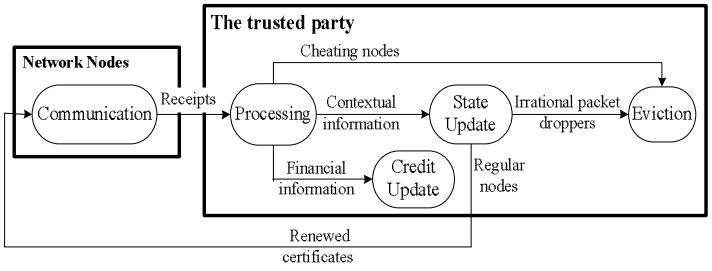


Fig. 2: The architecture of TRIPO.

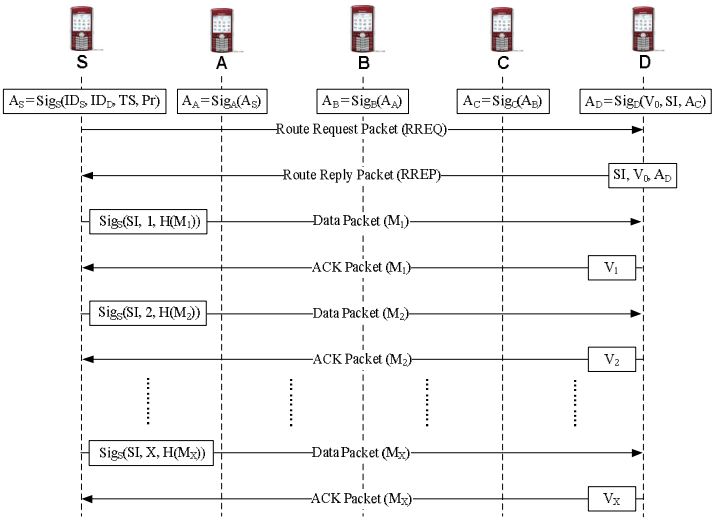


Fig. 3: The exchanged security tags in a session.

4. THE PROPOSED TRIPO

As shown in Fig. 2, TRIPO has four main phases. For *Communication Phase*, the nodes are involved in communication sessions and compose payment receipts. The nodes accumulate the receipts and submit them when the connection to TP is available. For *Processing Phase*, the TP processes the receipts to extract financial and contextual information and passes them to the *Credit Update Phase* and the *State Update Phase* to update the nodes' credit accounts and states. Once the RS identifies an irrational packet dropper, the TP evicts it by not renewing its certificate.

4.1 Communication Phase

4.1.1 Route Establishment

In order to establish an end-to-end route, the source node broadcasts the *Route Request Packet* (*RREQ*) that contains the identities of the source (ID_S) and the destination (ID_D) nodes, its certificate, time stamp (TS), the payment-splitting ratio (Pr), and its signature $A_S = Sig_S(ID_S, ID_D, TS, Pr)$. The source node is charged the ratio of Pr of the total payment and the destination node is charged the ratio of 1-Pr. After receiving the *RREQ* packet, a network node A signs the packet's signature to generate A_A, i.e., $A_A = Sig_A(A_S)$ as shown in Fig. 3. This signature authenticates node A and holds it accountable for dropping the next packets, i.e., the TP can make sure that node A indeed participated in the session. Then, node A broadcasts the *RREQ* packet after appending its identity (ID_A), certificate, and A_A.

The destination node receives *RREQ* packets for different routes to the source. If the verifications of the signatures of the first received *RREQ* packet, e.g., $A_C = Sig_C(Sig_B(Sig_A(Sig_S(ID_S, ID_D, TS, Pr))))$ in Fig. 3, fail, the destination node verifies the signatures of the second received *RREQ* packet and so on. In this way, if an intermediate node manipulates the *RREQ* packet, it cannot prevent establishing the session. The destination node generates a hash chain by iteratively hashing a random value V_S *S* times to obtain a final hash value V_0 called the root of the hash chain, where $V_{X-1} = H(V_X)$. The destination node signs the signature layers, V_0, and SI to generate the authentication code of the nodes in the session or A_D, e.g., $A_D = Sig_D(V_0, SI, A_C)$ in Fig. 3. SI contains the identities of the nodes in the session and TS, e.g., $SI = ID_S$, ID_A, ID_B, ID_C, ID_D, TS in Fig. 3. A_D can authenticate the nodes in the session with reduced packet overhead because it requires less space than attaching a separate signature for each node. A_D also authenticates the hash chain and links it to the session. The destination node sends back the *Route Reply Packet* (*RREP*) containing SI, V_0, its certificate, and A_D. After receiving the *RREP* packet, each intermediate node verifies A_D and relays the packet after adding its certificate. For example, node B authenticates S and A from the *RREQ* packet's signature (A_A) and authenticates C and D from the *RREP* packet's signature (A_D). The intermediate nodes store A_D, SI, and V_0 for composing the payment receipt.

4.1.2 Data Generation and Relay

As illustrated in Fig. 3, the source node appends the message M_X and its signature $Sig_S(SI, X, H(M_X))$ to the *X*th data packet,

where $H(M_X)$ is the hash value of M_X. Signing the hash of the message instead of the message can reduce the receipt size because the smaller-size $H(M_X)$ is attached to the receipt instead of M_X. Upon receiving the packet, each intermediate node verifies the source node's signature to ensure the message integrity and authenticity and verify the payment data that includes SI and X. The intermediate nodes save only the last received signature for composing the receipt because it is sufficient to prove transmitting *X* messages, e.g., after receiving the *X*th data packet, the intermediate nodes deletes $Sig_S(SI, X-1, H(M_{X-1}))$ and saves $Sig_S(SI, X, H(M_X))$.

4.1.3 ACK Generation and Relay

For each data packet, Fig. 3 shows that the destination node sends back *ACK* packet containing the pre-image of the last sent hash value from the hash chain. V_1 is released in the first *ACK* and V_2 in the second and so on. Each intermediate node verifies the hash values by making sure that V_{X-1} is obtained from hashing V_X. The payment approval and integrity can be ensured because the hash function is one-way, i.e., only the destination node can generate the hash chain. Therefore, instead of generating a signature per *ACK* to secure the payment, one signature is generated per *S ACK* packets. The nodes store only the last released hash value for the receipt composition. The number of delivered messages can be computed from the number of hashing operations to map V_X to V_0.

ISR(0)
D = SI, Pr, V_0
St = **H**(A_D)

a) The last received packet is *RREP*.

ISR(1)
D = SI, Pr, V_0, 1, $H(M_1)$,
St = **H**(Sig_S(SI, 1, $H(M_1)$), A_D)

b) The last received packet is M_1.

ISR(X)
D = SI, Pr, V_0, X, $H(M_X)$, V_{X-1}
St = **H**(Sig_S(SI, X, $H(M_X)$), A_D)

c) The last received packet is M_X and X > 1.

CSR(X)
D = SI, Pr, V_0, X, $H(M_X)$, V_X
St = **H**(Sig_S(SI, X, $H(M_X)$), A_D)

d) The last received packet is the ACK of M_X.

Fig. 4: The format of the session receipt.

4.1.4 Receipt Composition and Submission

When the session is completed or broken, each node in the session composes a receipt. It can be seen from Fig. 4 that a session receipt contains two main parts: *Descriptor (D)* and *Security Token (St)*. The *Descriptor* contains the session identifier, the number of messages (*X*), the hash value of the last message ($H(M_X)$), V_0, and the last hash value (V_X). The *Security Token* is a security proof that prevents payment repudiation and manipulation, and thus ensures that the receipt is undeniable, unmodifiable, and unforgeable. In order to reduce the receipt size, the *Security Token* is composed by hashing the signatures instead of attaching the signatures. Since the connection to the TP may not be available on regular basis, the nodes store the receipts and submit them in batch to the TP for redemption.

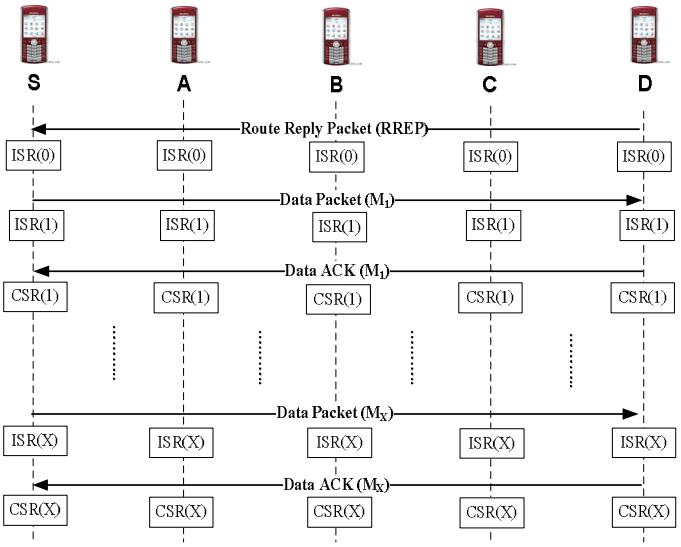


Fig. 5: The composed receipts when the last packet is data, ACK or RREP.

If a node drops the *RREP*, data, or *ACK* packets, the route is considered broken and re-established. As illustrated in Fig. 5, if the session is broken during relaying the *RREP* packet, the nodes that received the packet submit *Incomplete Session Receipt* (ISR(0)) to enable the RS to identify the attackers that frequently drop the *RREP* packets. The format of the ISR(0) is shown in Fig. 4(a). If the session is broken during relaying the *X*th data packet, the nodes that received the packet submit the *Incomplete Session Receipt* for *X* packets or ISR(X). In Fig. 4(b), ISR(1) does not contain V_1 because the first *ACK* packet is not received. In Fig. 4(c), for $X > 1$, ISR(X) contains the source node's signature for *X* messages, but the last released hash value is V_{X-1} instead of V_X because the *ACK* of the *X*th message is not received. This receipt is called "*Incomplete Session*" because it is submitted only when the session is broken. Submitting ISR(X) by node C entails that the node has successfully relayed *X*-1 packets and received one, but it is clear that all the nodes before C in the session (A and B) have indeed relayed the *X*th data packet. If the last received packet is the *X*th *ACK*, the nodes submit the *Complete Session Receipt* or CSR(X). Fig. 4(d) shows that CSR(X) contains the source node's signature for X packets and V_X that is a proof of receiving the *X*th *ACK*. This receipt is called "*Complete Session*" because the session is complete if all the nodes in the session submit CSR(X).

4.2 Processing Phase

Once the TP receives the receipts of a session, it first uses the session's unique identifiers (SI) to make sure that the receipts have not been processed before. Then, to verify the cre-

dibility of the receipts, the TP creates the receipt's *Security Token* by generating the nodes' signatures and hashing them. The receipt is credible if the resultant hash value is identical to the receipt's *Security Token*. The TP verifies the destination node's hash chain by making sure that V_0 is obtained from hashing V_X X times. The TP processes the receipts to extract the financial and the contextual information. The financial information includes who pays whom and how much, and the contextual information reflects the nodes' misbehaviors in terms of payment cheating and packet dropping. This information is called contextual because it is not carried in the receipts but extracted from the context of the receipts such as the format (ISR or CSR) and the number of messages. The TP classifies each session into fair or cheating, and the fair sessions are further classified into complete or broken. A fair session is complete when the source node transmits its last message, but it is broken when at least one link is broken during transmitting the data, *ACK*, or *RREP* packets. For cheating session, at least one node does not submit the receipt or submits tampered receipt for rational reasons such as paying less or for irrational reasons to circumvent the RS.

A session is complete when all the nodes in the session submit *Complete Session Receipts* for the same number of packets or CSR(X). For the broken sessions, there are only four possible cases shown in Fig. 6. The TP can identify the broken link from the format of the receipts and/or the number of messages. In Fig. 6(a), if the link between nodes A and B is broken during relaying the *RREP* packet, the nodes from B to D submit ISR(0), but the nodes from S to A do not submit receipts. Since node A may drop the *RREP* packet but does not submit the receipt to circumvent the RS, the system accuses the two nodes in the broken link of dropping the packet. In Section 4.4, we will discuss how the RS can precisely differentiate between the honest nodes and the irrational packet droppers. In Figs. 6(b, c), the link between nodes B and C is broken during relaying the Xth data packet. If $X = 1$, the nodes B and C submit ISR(1) and ISR(0), otherwise they submit ISR(X) and CSR(X-1), respectively. In Fig. 6(d), the link between nodes A and B is broken during relaying the *ACK* of M_X, so they submit ISR(X) and CSR(X), respectively.

The TP classifies a session into cheating if it is not complete or broken. Without loss of generality, Table 3 gives numerical examples for cheating sessions. For Case 1, the source node submits receipt with smaller number of messages to pay less because the intermediate and destination nodes cannot compose CSR(5) without the signature of the source node for five messages. For Case 2, the source and destination nodes collude to submit receipts with less payment because the intermediate nodes cannot compose their receipts without the signature of the source node for seven messages and V_7. As shown in Fig. 2, the nodes that submit incorrect receipt such as node S in Case 1 and S and D in Case 2 are evicted. For Case 3, node A cannot compose its receipt without the signature of the source node for four messages and V_4. For Case 4, the receipt of node B is not consistent with the receipts of the other nodes. Node B may drop the 9th data packet and submit less-payment receipt to circumvent the RS, or the other nodes collude to accuse node B of cheating. For Case 5, the source and the destination nodes may collude to create receipts for more messages, but they cannot fabricate receipts for fake sessions to falsely accuse nodes of dropping packets because the signatures of the intermediate nodes are required to compose valid receipt, which is important to make *False-Accusation* attack difficult. *The only way the attackers can falsely accuse an honest node of dropping packets is by neighboring the node and dropping packets or by paying more credits by submitting receipts for more messages such as Cases 4 and 5*. For Case 6, node B dropped the 6th data packet and does not submit the receipt, or the other nodes collude to falsely accuse node B, but the colluders have to neighbor node B to compose valid A_D that contains the signature of node B and use A_D to compose valid receipts.

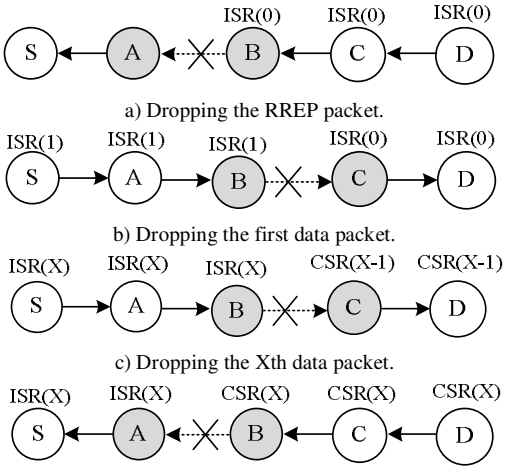


Fig. 6: The possible cases for dropped packets.

TABLE 3: NUMERICAL EXAMPLES FOR CHEATING SESSIONS.

Case	S	A	B	C	D
1	CSR(3)	CSR(5)	CSR(5)	CSR(5)	CSR(5)
2	CSR(6)	CSR(7)	CSR(7)	CSR(7)	CSR(6)
3	--	CSR(4)	--	--	--
4	ISR(9)	ISR(9)	CSR(3)	CSR(8)	CSR(8)
5	CSR(6)	CSR(5)	CSR(5)	CSR(5)	CSR(6)
6	ISR(6)	ISR(6)	----	CSR(5)	CSR(5)

4.3 Credit-Account Update Phase

The AC clears the receipts of the fair sessions according to the charging and rewarding policy discussed in Section 3.3. For the cheating sessions, the AC clears the receipts in such a way that prevents stealing credits and punishes the cheating nodes to discourage cheating actions. For example, Cases 1 and 2 in Table 3 are cleared for five and seven messages, respectively because it is obvious that S cheats in Case 1 and S and D cheat in Case 2. For Case 3, node A is rewarded for four messages, nodes B and C are not rewarded because they do not submit the receipt, and S and D are charged for four messages. For Cases 4 to 6, each node is rewarded or charged according to the payment of its receipt, so the payee that does not submit a receipt is not rewarded, the payee that submits less-payment receipt is rewarded less, and the payers that submit more-payment receipts are charged more. In this way, *the nodes that submit incorrect receipts always lose credits*.

4.4 State Update Phase

As shown in Fig. 2, the contextual information is used to update the nodes' reputation values to identify the irrational packet droppers. The RS performs the following three processes: (1) In *Rating Calculation*, a rating is calculated for each node in a session; (2) In *Reputation Update*, a node's reputation value is updated by aggregating its session rating with its old reputation value; and (3) In *State Update*, once a node's reputation value reaches to a threshold, the node is identified as irrational packet dropper and evicted.

4.4.1 Rating Calculation

A node's rating is the probability that the node drops packets in a session, so the nodes that are not in a broken link receive positive rating (0) because they cannot be packet droppers. In other words, all the nodes in complete sessions receive positive ratings, and the nodes that are not in the broken link of a broken session receive positive ratings. For the Cases 4 to 6 in Table 3, all the nodes receive negative ratings of (1), and thus *if an attacker manipulates its receipts, he loses credits and also receives negative ratings.* For the two nodes in a broken link, two techniques are proposed to calculate their negative ratings, called *Simple* and *Weighted Rating Techniques*.

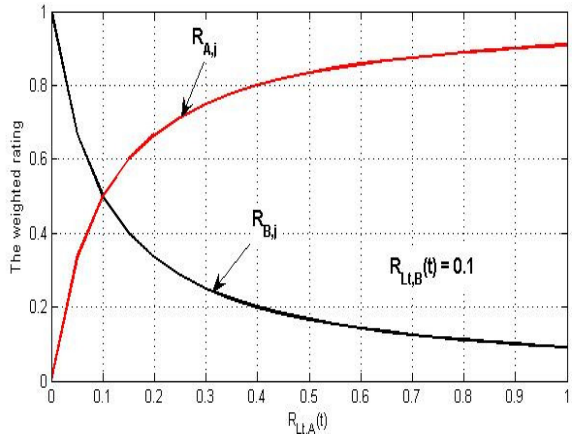
A. Simple Rating Technique (SRT)

The two nodes in a broken link receive equal negative ratings of (1), i.e., the two nodes are equally accused of dropping the packets regardless of their history of dropping packets. The rationale of this technique is that *the irrational packet droppers should be involved in much more broken links than the honest nodes to launch effective attacks, so they can be identified because they collect much more negative ratings.* The technique is called simple because it requires simple computations and small storage area.

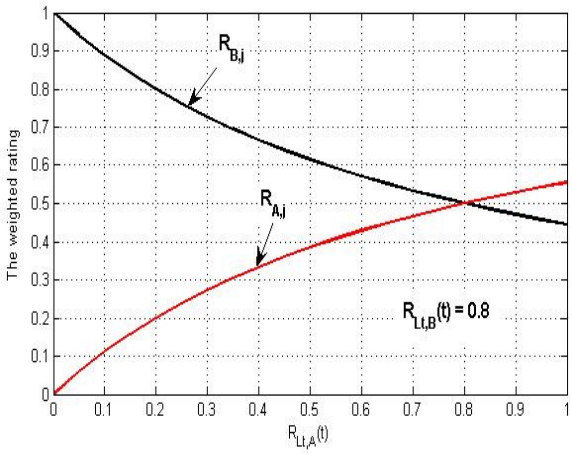
B. Weighted Rating Technique (WRT)

The two nodes in a broken link receive ratings that are proportional to their frequency of dropping packets in the past. If the link between two neighboring nodes A and B is broken in session j, Eq. 1 is used to calculate the rating of A ($R_{A,j}$) which is the reputation value of node A ($R_{Lt,A}(t)$) to the summation of the two nodes' reputation values. By the same way, the rating of node B ($R_{B,j}$) is its reputation value to the summation of the two nodes' reputation values, or ($R_{B,j}$ = 1-$R_{A,j}$). As shown in Fig. 7, if nodes A and B have the same reputation value ($R_{Lt,A}(t)$ = $R_{Lt,B}(t)$), they receive equal negative ratings of 0.5, but the node with worse (higher) reputation value receives more negative rating and vice versa. *The rationale of this technique is that the worse-reputation node is more likely the packet dropper because it has been involved in more broken links.* The main advantage of WRT is that *if an honest node and an irrational packet dropper are involved in a broken link, they receive low and high negative ratings, respectively, which enables the RS to precisely differentiate between the honest nodes and the irrational packet droppers because the reputation values of the irrational packet droppers degrade much faster than those of the honest nodes do.* In other words, the irrational packet droppers cannot cause big reduction in the reputation values of the honest nodes, but the honest nodes can cause big reduction in the reputation values of the irrational packet droppers.

$$R_{A,j} = \frac{R_{Lt,A}(t)}{R_{Lt,A}(t) + R_{Lt,B}(t)} \quad (1)$$



a) B is an honest node.



b) B is an irrational packet dropper.

Fig. 7: The weighted ratings of two nodes in a broken link.

In Fig. 7(a), B is an honest node because its reputation value is low. If node A is also honest, e.g., with a reputation value between 0.05 and 0.15, the two nodes receive ratings between 0.4 and 0.6. However, if node A is an irrational packet dropper, e.g., with a reputation value of 0.8, nodes A and B receive ratings of 0.89 and 0.11, respectively. In Fig. 7(b), node B is an irrational packet dropper with a reputation value of 0.8. If node A is also irrational packet dropper with a reputation value close to 0.8, the ratings of the two nodes is around 0.5. In other words, an irrational packet dropper receives less and more negative ratings when it neighbors irrational packet droppers and honest nodes, respectively, so an irrational packet dropper can be identified in shorter time when it neighbors honest nodes more because its reputation value degrades faster. Due to this property, *if the number of honest nodes is larger than the number of irrational packet droppers, WRT can accelerate the degradation of the irrational packet droppers' reputation values*, i.e., the well-behaving majority can kick out the misbehaving minority.

4.4.2 Reputation Update

Using a reputation system is necessary to keep track of the nodes' long-term packet dropping activities because packets may be dropped for non-malicious reasons, e.g., due to mobility, or temporarily, e.g., due to network congestion, but the high frequency of dropping packets is an obvious misbehavior. The RS computes a reputation value for each node by accumulating its ratings. A node's rating is the probability that a node drops packets in one session, but the reputation value is an evaluation to the node's packet dropping activities over a large number of sessions. In Fig. 8, the RS stores a rating window for the latest γ ratings of node A, where $R_{A,j}$ is the rating of node A in session number j, and $R_{A,j} \in \{0, 1\}$ and [0, 1] in SRT and WRT, respectively. After computing a new rating, the rating window is shifted to right to cancel the oldest rating ($R_{A,j}$), and the new rating is stored at right. Then, with Eq. 2, the short-term reputation value ($R_{St,A}(t)$) is calculated by averaging the latest γ ratings, which is an evaluation to the node's packet dropping activities in the latest γ sessions. Finally, with Eq. 3, the new long-term reputation value ($R_{Lt,A}(t)$) is calculated by aggregating $R_{St,A}(t)$ with the old long-term reputation ($R_{Lt,A}(t\text{-}1)$), where $R_{St,A}(t)$, $R_{Lt,A}(t)$, and $\alpha \in [0, 1]$. $R_{Lt,A}(t)$ expresses the probability that node A is an irrational packet dropper, i.e., $R_{Lt,A}(t)$ should be large for the irrational packet droppers. α is called fading factor that determines the given weight to the nodes' past packet dropping events. The value of α determines how fast the long-term reputation value builds up and falls down, i.e., the lower value α is, the faster the old reputation value is forgotten, and vice versa. In order to improve the effectiveness of the reputation system, α should be greater than 1-α because $R_{Lt,A}(t\text{-}1)$ is calculated over more sessions than $R_{St,A}(t)$.

A node's reputation value is updated by $R_{St,A}(t)$ instead of only the latest rating (good or bad) to precisely differentiate between the honest and the irrational packet droppers. In this way, *the long-term reputation values of the honest nodes degrade slower than those of the irrational packet droppers do because their short-term reputation values are smaller*. By the same way, *the long-term reputation values of the honest nodes improve faster than those of the irrational packet droppers do when they receive positive ratings because the honest nodes' short-term reputations are smaller*. Moreover, the honest nodes can filter out their negative ratings in two levels: shifting the rating window forgets the node's behavior in one session, and using α forgets a ratio of the node's past behavior.

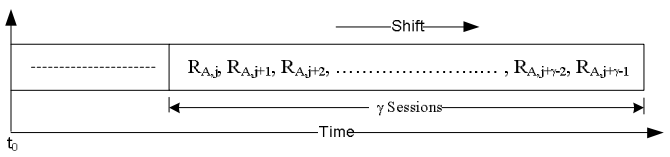


Fig. 8: The rating window of node A contains its latest γ ratings

$$R_{St,A}(t) = \frac{1}{\gamma} \cdot \sum_{k=1}^{\gamma} R_{A,k} \quad (2)$$

$$R_{Lt,A}(t) = \alpha \cdot R_{Lt,A}(t-1) + (1-\alpha) \cdot R_{St,A}(t) \quad (3)$$

4.4.3 State Update

A node's state is a conclusion for its behavior based on the accumulated experience on it (or its reputation value), which can be an expectation to its behavior in the future. A node's state space includes three mutually disjoint states: honest or regular node (+1), suspicious or undecided (0), and evicted (-1). From Eq. 4, the state of node A ($S_A(t)$) is honest if the node's long-term reputation value is below the honest threshold R_h; $S_A(t)$ is evicted if the node's long-term reputation value is above the malicious threshold R_m; otherwise, $S_A(t)$ is suspicious. Moreover, a node is identified as irrational packet dropper and evicted when it spends ω consecutive sessions in the suspicious state because the node receives negative ratings more than the normal rate. A node is also evicted when the difference between the spent times in the honest and the suspicious states is less than β because the node receives positive ratings less than the normal rate.

$$S_A(t) = \begin{cases} +1, & R_{Lt,A}(t) < R_h \quad \text{(Honest)} \\ 0, & R_h \le R_{Lt,A}(t) \le R_m \quad \text{(Suspicious)} \\ -1, & R_{Lt,A}(t) > R_m \quad \text{(Evicted)} \end{cases} \quad (4)$$

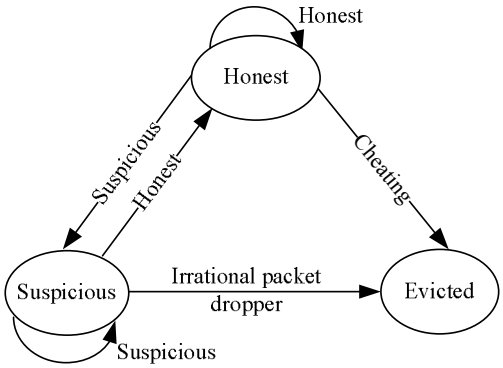


Fig. 9: A node's state transition diagram.

The state transition diagram of a node is shown in Fig. 9. Suspicious node may be honest but its reputation value is temporarily degraded, so instead of taking a harsh reaction by characterizing this node as irrational packet dropper, the RS collects more information about the node's behavior to figure out whether its misbehavior is temporary or genuine. If a suspicious node is honest, it should be able to improve its reputation value and return to the honest state, but the irrational packet dropper stays for some time in the suspicious state before being evicted. As shown in the figure, a node is transferred directly from the honest to the evicted state without passing through the suspicious state when it commits a clear cheating action such as node S in Case 1 in Table 3. R_m can reveal the attackers that drop packets more than the normal rate, β can reveal the attackers that drop packets in a large number of consecutive sessions such as broken nodes that misbehave after gaining good reputation, and ω can reveal the attackers that spend long time in the suspicious state such as *Gray-Hole* attackers. Since we cannot know whether a packet is dropped due to non-malicious reasons or intentionally, the attackers may drop packets with keeping their reputations above the thresholds of the reputation

system to avoid eviction. If the thresholds are close enough to the normal rate, the reputation system can force the attackers to drop packets at a lower rate than the system's thresholds, i.e., *the RS can force the smart attackers to behave in such a way that is not severe threat to the network proper operation.* R_h enables an honest node to filter out its negative ratings because the node is identified honest as long as its reputation value is less than R_h. The system tolerates the degradation of a node's reputation value up to R_m provided that the node improves its reputation and returns to the honest state.

5. Security Analysis

5.1 Defense against Payment Manipulation

For *Double-Rewarding* attack, the attacker attempts to clear a receipt multiple times to increase its rewards. TP can thwart the attack and identify the attacker because each receipt has unique identifier (SI). For *Double-Spending* attack, the attacker attempts to generate identical receipts for different sessions to pay once. In TRIPO, a session's identifier is unrepeatable because it contains the identities of the nodes in the route and time stamp. For *Receipt-Forgery-or-Manipulation* attack, the attackers attempt to forge receipts or manipulate valid receipts to increase their rewards. This is impossible in TRIPO with using secure hash function and public-key cryptography because it is not possible to forge or modify the nodes' signatures, compute the hash value of the signatures without computing the signatures, and compute V_X from V_{X-1}. For *Free-Calling (or Riding)* attacks, two colluding intermediate nodes in a legitimate session manipulate the session packets to add their data to communicate freely. To thwart this attack, the integrity of the packets should be checked at each node, and thus the first node after the colluder can detect the packet manipulation and drop the packet. For the data, *RREQ*, and *RREP* packets, the nodes' signatures can ensure the integrity of the packets. The integrity of the *ACK* packets can also be ensured by verifying the hash chain elements.

For *Packet-Replay* attack, the internal or external attacker record valid packets and replay them in different place and/or time to establish sessions under the name of others to communicate freely. To thwart this attack, a fresh time stamp is used to establish a session to ensure that stale packets can be identified and dropped. For *Impersonation* attack, the attackers impersonate legitimate nodes to communicate freely or steal credits. This attack is not possible because the nodes use their private keys to sign the packets. For *Reduced-Payment* attack, some intermediate nodes may collude with the source and destination nodes to submit receipts with less payment. In TRIPO, even if a group of nodes colludes to reduce the rewards of an honest node, the node can submit a receipt with the correct payment, such as Cases 1 to 3 in Table 3. For *Receiver-Robbery* attack, the colluding nodes attempt to steal credits from the destination node by sending bogus messages that the destination node pays for them. In TRIPO, the intermediate nodes are rewarded only when the destination node acknowledges receiving correct data, and a route cannot be established if the destination node is not interested in the communication because its signature is required.

5.2 Defense against Irrational Packet Dropping Attack

Unlike the cooperation enforcement mechanisms that may not have sufficient time to judge the nodes' real behavior due to the nodes' mobility, TRIPO can monitor the nodes over different sessions and long time to precisely identify their behaviors. Moreover, packet drop is beneficial for the nodes in cooperation enforcement mechanisms because packet relay consumes their resource without benefits, but packet relay is beneficial for the nodes in TRIPO to earn credits. In TRIPO, singular attackers cannot launch *Reputation-Boost* attacks, and they have to neighbor the victim nodes and drop packets to launch *False-Accusation* attacks. First, neighboring the victim nodes may not be easy due to the nodes' mobility; second, the attackers also receive negative ratings and falsely accusing a node does not guarantee that this accusation will be effective because the node can filter out its negative ratings; finally, frequently launching *False-Accusation* attack reduces the effectiveness of the attack with using WRT because the honest nodes and the attackers receive less and more negative ratings, respectively, which also makes it difficult for an attacker to play with multiple identities to launch stronger attacks. Although the honest nodes may receive negative ratings when they neighbor irrational packet droppers, the neighbors change due to node mobility, which can distribute the negative ratings instead of concentrating them on few nodes. Moreover, since dropping the *RREQ* packets is not abuse, an honest node can protect its reputation value by not involving itself in sessions with the neighbors that frequently drop packets.

Reputation systems are susceptible to collusion attacks due to the nature of these systems. The impact of small-scale collusion attacks can be mitigated by categorizing ratings by identities. The system can construct neighbor density table (NDT) for the negative and positive ratings of a node's rating window. The density of the negative (or positive) ratings of node B in the NDT of node A is the number of negative (or positive) ratings that are caused when B was neighbor to A to the total number of negative (or positive) ratings in the rating window of node A, i.e., the density of the negative (or positive) ratings reflects the frequency that node B caused negative (or positive) ratings to node A. Obviously, in small-scale collusion attack, the colluders have much higher densities than the other nodes. Investigating the NDT in deciding a node's state can improve the mechanism's robustness. For example, in *Reputation-Boost* and *False-Accusation* attacks, few nodes have high densities in a node's positive and negative ratings, respectively, and the node's reputation value becomes bad and good with excluding these false ratings, respectively. NDT can prevent a small number of colluders from falsely improving their reputation values and evicting honest nodes from the network, and thus forces the attackers to collude with a large number of nodes, which is not easy in civilian and large-scale networks [31], [32]. Certainly, if the densities of the NDT are flat or dominated by a large number of nodes, the RS can have a strong belief about the node's real behavior. Several measures can be taken to improve the robustness against large-scale collusion attacks. Clearance fees can be imposed to clear the payment of a session to discourage submitting receipts for fake sessions to

launch *Reputation-Boost* attack. If colluders tamper their receipts to accuse a victim, they lose credits and defame their reputation values, e.g., Cases 4 to 6 in Table 3.

Eq. 5 gives the probability that a node receives at least a ratio of R_m negative ratings in γ sessions, or the probability of identifying a node as irrational packet dropper, where P is the probability of receiving a negative rating in a session. Obviously, P should be much larger for packet droppers than the honest nodes because they drop much more packets. Fig. 10 shows that if $R_m \in [0.35, 0.55]$, the reputation system can perfectly differentiate between the honest nodes and the irrational packet droppers. However, if R_m is low, e.g. [0, 0.35), honest nodes may be falsely identified as packet droppers, and if R_m is too tolerant, e.g. (0.55, 1], packet droppers may not be identified. Thus, R_m can control the tradeoff between the false accusation probability and the probability of identifying the packet droppers. The increase of P increases $P_i(\gamma)$ at the same R_m, and thus some honest nodes may be falsely identified as packet droppers if R_m does not have enough tolerance.

$$P_i(\gamma) = \sum_{k=\gamma.Rm}^{\gamma} \binom{\gamma}{k} \cdot P^k \cdot (1-P)^{\gamma-k} \quad (5)$$

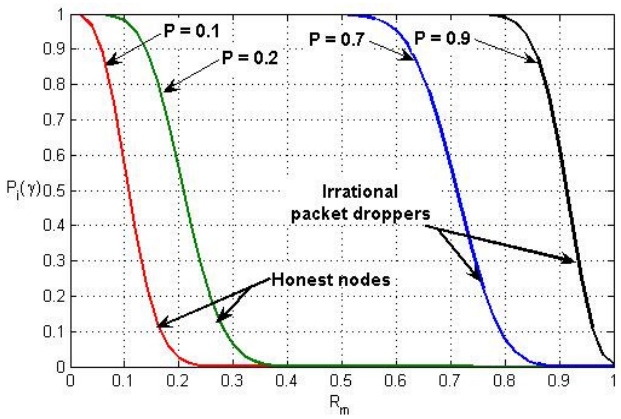


Fig. 10: The effect of Rm on the reputation system at $\gamma = 50$.

From Fig. 11, increasing the size of γ increases $P_i(\gamma)$ of the irrational packet droppers and decreases $P_i(\gamma)$ of the honest nodes, which can reduce the number of honest nodes that are falsely identified as packet droppers and the number of irrational packet droppers that are not identified. For example, if $R_m \in [0.3, 0.7]$ and $\gamma = 10$, some honest nodes may be falsely identified as packet droppers and some irrational packet droppers may not be detected, but the RS can perfectly identify the nodes' behaviors when $\gamma = 100$ or 250. However, this does not mean that the RS has to wait long time until the nodes participate in γ sessions for identifying the irrational packet droppers because a node's rating window is not empty when the node first joins the network but has initial value. From Fig. 12, the aggressive attackers that drop packets with very high rate, i.e., having large P, can be identified after participating in a low number of sessions (or shorter time). For example, the probabilities to identify the irrational packet droppers after participating in 20 sessions are 0.87, 0.92, and 0.96 for P of 0.6, 0.63, and 0.66 respectively.

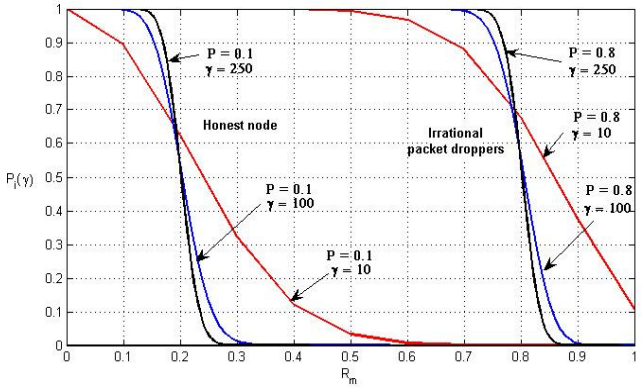


Fig. 11: The effect of γ on the reputation system.

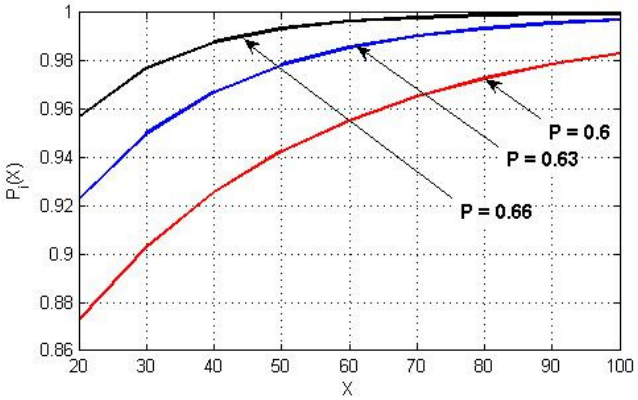


Fig. 12: The effect of P on $P_i(X)$ at Rm = 0.5.

In order to evaluate the overhead and the effectiveness of TRIPO, a network simulator is programmed using MATLAB. 35 mobile nodes with 125 m radio transmission range are randomly deployed in a square cell of 1000 m by 1000 m. We adopt the modified random waypoint model [33] to emulate the nodes' mobility. Specifically, a node travels towards a random destination uniformly selected within the network field; upon reaching the destination, it pauses for some time; and the process repeats itself afterwards. The node speed is uniformly distributed in the range [0, 10] m/s and the pause time is 10 s. The constant-bit-rate traffic source is implemented in each node as an application layer, and the source and destination nodes are randomly chosen. The DSR routing protocol [29] is simulated over distributed coordination function of the IEEE 802.11 medium access control protocol. The time stamp (TS), a node's identity (ID_A), and the number of messages (X) are five, four, and two bytes, respectively. 300 sessions are held in each updating time, packet transmission rate is 0.5 packets per second, and 25 packets are transmitted in each session if the route is not broken. To determine proper thresholds, we run a training phase assuming that all the nodes are honest to investigate the expected and tolerable ratio of dropping the packets. The parameters R_h, ω, β, γ, and α are 0.19, 100, 100, 50, and 0.78, respectively. The initial rating window is the repeat of the pattern '00001', so the nodes' initial reputation values and states are 0.2 and honest, respectively.

In Table 4, the number of false-positive nodes is the average number of honest nodes that are falsely identified as irrational packet droppers, and the detection time is the average number of updating times for identifying all the irrational packet drop-

pers. The attack strength 1:X means that the attackers behave as irrational packet droppers in one session and behave normally in X-1 sessions to circumvent the RS. However, the attacker has to drop a large ratio of the packets to launch effective attacks, i.e., X should be small. When X = 1, the attackers launch *Black-Hole* attacks by dropping all the packets they should relay, otherwise they launch *Gray-Hole* attacks. The simulation results given in Table 4 can demonstrate the intuitive tradeoff between the detection time and the number of false positive nodes, which can be controlled by R_m. Less tolerance to the negative ratings (R_m = 0.35) shortens the detection time but increases the number of false-positive nodes. This tradeoff is sharper in SRT than WRT because the honest nodes collect more negative ratings. It takes longer to identify the nodes that misbehave less frequently such as the attackers with 1:2 attacking strength because they lose their reputation values slowly. The increase of the ratio of the attackers increases the number of false-positive nodes because the honest nodes collect more negative ratings due to neighboring more attackers, and the victims could not improve their reputation values with the same rate they degrade. Nevertheless, for R_m = 0.35 and X = 1, when a large ratio of 42.86% (16 nodes) of the nodes drop all the packets they should relay, almost no node is falsely accused in WRT but around 13.25 nodes (37.8%) are falsely accused in SRT. That is because honest nodes receive less negative ratings in WRT, i.e., *WRT can better filter out the negative ratings of the honest nodes, which is important to precisely identify the irrational packet droppers.*

The number of false-positive nodes can be reduced in SRT with increasing R_m, e.g., for X = 1 and 42.86% of the nodes are attackers, the increase of R_m from 0.35 to 0.6 reduces the number of false-positive nodes from 13.35 (37.8%) to 2.8 (8%). However, the increase of R_m means that the attackers can drop more packets with keeping their reputation values above the system thresholds and the detection time increases. *R_m can be less in WRT, e.g., R_m = 0.35, for short detection time and low number of false-positive nodes because the attackers and the honest nodes collect more and less negative ratings, respectively comparing with SRT.* Moreover, the simulation results demonstrate that the increase of the number of attackers increases the detection time because some attackers may not participate in any sessions in an updating time, and the attackers receive less negative ratings due to neighboring more attackers and fewer honest nodes in WRT. In addition, the number of false-positive nodes increases with reducing γ, which confirms our observation in Fig. 11.

Since the thresholds of the reputation system have direct impact on the system's effectiveness, our centralized reputation system can compute good thresholds from the nodes' reputation values and periodically tune them. For example, if the reputation values of the majority of the nodes are less than 0.3, R_h can be decided as 0.3 assuming that the majority of the nodes behave honestly. Moreover, since the nodes contact the TP over discrete times, the detection and eviction times can be reduced with issuing shorter-lifetime certificates to the bad-reputation nodes. Moreover, investigating the rate of change of the reputation values can reduce the detection time for some attackers, e.g., this rate of change is larger for the *Gray-Hole* attackers than the honest nodes.

TABLE 4: SIMULATION RESULTS.

Attack strength	R_m	Attackers' ratio	Detection time (in updating times)		Number of false-positive nodes (γ = 50)		Number of false-positive nodes (γ = 15)	
			SRT	WRT	SRT	WRT	SRT	WRT
1:1	0.35	5%	1	1.85	2.8	0	8.85	0.16
		42.86%	1.9	4.4	13.35	0.1	16.17	0.56
	0.6	5%	2.25	14	0	0	0.9	0
		42.86%	5.3	98	0.85	0	2.85	0
1:2	0.35	5%	1.15	10.95	3.6	0	11.35	0.72
		42.86%	2	23.65	10	0	12.6	2.24
	0.6	5%	38.8	102.85	0	0	1.75	0
		42.86%	95.75	109.8	0.2	0	5.95	0

6. PERFORMANCE EVALUATION

Packet-Dropping attack degrades the network performance significantly. From [7] and [8], the average throughput degrades by 16% to 32% if 10% to 40% of the nodes drop packets, and the end-to-end packet delay linearly increases with the increase of the number of attackers. Moreover, since a new receipt is generated when the session is broken and re-established, *Packet-Dropping* attack increases the number of receipts. The attack also wastes the consumed energy and bandwidth in transmitting the packet from the source to the attacker. A packet cannot reach to its destination if any intermediate node drops the packet, and thus the packet delivery ratio (PDR) decreases with the growth of the number of attackers. Eq. 6 gives the probability of dropping a packet by an irrational packet dropper in a session with n nodes (or n-2 intermediate nodes). P_m is the ratio of the irrational packet dropper, which is equivalent to the probability that an intermediate node is an irrational packet dropper. The packet delivery ratio of a route with n nodes (PDR(n)) is the number of delivered data packets to the number of sent packets in the route. In Eq. 7, PDR(n) and $PDR_0(n)$ are the average packet delivery ratios of a route with n nodes with and without the irrational packet droppers, respectively. *Fig. 13 shows that a low ratio of irrational packet droppers as 20% can reduce the packet delivery ratio by 74% and 60% for routes with eight and six nodes, respectively.* Moreover, the increase of n or P_m increases the packet dropping probability and thus degrades the PDR.

$$P_b(n) = 1 - (1 - P_m)^{n-2} \quad (6)$$

$$PDR(n) = PDR_0(n) \cdot (1 - P_b(n)) \quad (7)$$

Public-key cryptography is necessary for securing the wireless networks [12], [13]. TRIPO uses public-key cryptography to enable the TP and the intermediate nodes to verify the payment. Instead of generating a signature per *ACK* packet, a hash chain is used to reduce the number of public-key-cryptography operations. The proposed communication protocol in [20] can be used with TRIPO to replace the source node's signatures with hashing operations. Digital signature technology and

hardware implementation have been improved and fast signature schemes are currently available. For example, "on-line/offline" digital signature [34] is computed in two steps: an off-line step that is computationally more demanding and independent of the message is performed before the message to be signed is available; and a lightweight on-line step is performed once the message to be signed becomes available. Moreover, the FPGA implementation of the RSA signature scheme can perform the signing and verifying operations in several milliseconds [35]. In route establishment, the nodes in the route use signatures to authenticate themselves not only to secure TRIPO by holding the nodes accountable for dropping packets but also to thwart many attacks that can be launched by external attackers (that are not members in the network) [36]. For example, the external attackers may launch *Resource-Exhaustion* attacks by frequently flooding the network with *RREQ* packets to exhaust the nodes' resources. In this authentication process, each node performs one signing operation and multiple verifying operations, and thus RSA signature scheme may be a proper choice because the verifying operations require much less computational time and energy than the signing operations [37]. Moreover, dropping the data packets is more serious than dropping the *RREP* packets because they are much longer, so the number of public-key-cryptography operations and receipts can be significantly reduced if TRIPO aims to identify only the data-packet droppers. In this case, ISR(0) receipts are not submitted, and the nodes can authenticate themselves in the *RREP* packets in order to reduce the number of public-key-cryptography operations because the *RREP* packets are processed only by the nodes in the route.

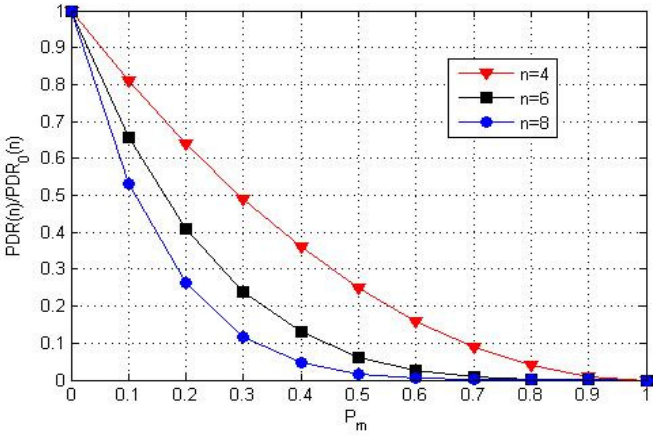


Fig. 13: The expected drop in the PDR due to irrational packet dropping attacks.

The simulation results show that the average receipt size is 126.6 bytes using SHA-1 hash function with digest value of 20 bytes [38]. The ratings of SRT and WRT are stored in one and seven bits, respectively, and thus a rating window for 320 ratings requires storage area of 40 and 280 bytes, respectively. Moreover, the storage area can be significantly reduced by making the size of the rating window dynamic. The rating windows can be short for the good-reputation nodes and long for the bad-reputation nodes, e.g., suspicious nodes, to better judge their behavior. In addition, the overhead of TRIPO can be significantly reduced by running the reputation system only on-demand when TP notices that the packets are dropped more than the normal rate, and the system can be run only for the suspected nodes that are frequently involved in broken links.

7. Conclusion and Future Work

In this paper, we have proposed a novel mechanism that adopts stimulation and punishment strategies to thwart *Packet-Dropping* attack in multihop wireless networks. Credits are used to stimulate the rational packet droppers to relay others' packets and the payment receipts can be processed to detect the broken links to build a reputation system to identify the irrational packet droppers. SRT offers equal negative ratings to the two nodes in a broken link but WRT offers more negative rating to the node that dropped more packets in the past. Our analytical and simulation results demonstrate that our mechanism can secure the payment against singular and colluding attackers. Moreover, WRT can precisely identify the irrational packet droppers with almost no false-positive nodes. The reputation system is secure against small-scale irrational collusion attacks and robust against large-scale collusion attacks because the attackers lose credits and defame their reputations.

The honest nodes have different packet-dropping rates, i.e., the nodes with large hardware-capability and low mobility have less packet-dropping probability. In our future work, we will develop a routing protocol to route traffic through the nodes having low packet-dropping probability to integrate the nodes' past behavior into routing decisions as a second line of defense against *Packet-Dropping* attack and to improve route stability and thus the network performance. In addition, in order to reduce the overhead of submitting and clearing the receipts, each node can store the receipts' and *Security Token* and submits only lightweight payment reports containing the alleged charges and rewards. A security mechanism will be developed to request the and *Security Token* when the nodes' reports are not consistent to identify the cheating nodes. The mechanism should thwart different cheating strategies to secure the payment.

References

[1] G. Shen, J. Liu, D. Wang, J. Wang, and S. Jin, "Multi-hop relay for next-generation wireless access networks", Bell Labs Technical Journal, vol. 13, no. 4, pp. 175-193, 2009.

[2] Y. Bi, L. X. Cai, X. Shen, and H. Zhao, "Efficient and reliable broadcast in inter-vehicle communications networks: A cross layer approach", *IEEE Trans. on Vehicular Technology,* vol. 59, no. 5, pp. 2404-2417, 2010.

[3] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications", IEEE Trans. on Vehicular Technology, vol. 59, Issue 7, pp. 3589-3603, 2010.

[4] P. Gupta and P. Kumar, "The capacity of wireless networks", IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388-404, March 2000.

[5] 3rd Generation Partnership Project, Technical Specification Group Radio Access Network, "Opportunity driven multiple access", 3G Technical Report 25.924 version 1.0.0, December 1999.

[6] M. Mahmoud and X. Shen, "Credit-based mechanism protecting multi-hop wireless networks from rational and irrational packet drop", Proc. of IEEE GLOBECOM'10, Miami, Florida, USA, December 6-10, 2010.

[7] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", Proc. of ACM Mobile Computing and Net-

working (MobiCom'00), pp. 255–265, Boston, Massachusetts, USA, August 6-11, 2000.
[8] P. Michiardi and R. Molva, "Simulation-based analysis of security exposures in mobile ad hoc networks", Proc. of European Wireless, Florence, Italy, February 25–28, 2002.
[9] J. Hu, "Cooperation in mobile ad hoc networks", Technical report (TR-050111), Computer Science Department, Florida State University, Tallahassee, January 2005.
[10] G. Marias, P. Georgiadis, D. Flitzanis, and K. Mandalas, "Cooperation enforcement schemes for MANETs: A survey", Wiley's Journal of Wireless Communications and Mobile Computing, vol. 6, issue 3, pp. 319–332, 2006.
[11] G. Iannaccone, C. Chuah, R. Mortier, S. Bhattacharyya, and C. Diot, "Analysis of link failures in an IP backbone", Proc. of IMW 2002, ACMPress, Marseille, France, November 2002.
[12] K. Sanzgiri, D. LaFlamme, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "Authenticated routing for ad hoc networks", IEEE Selected Areas in Communications, vol. 23, no. 3, pp. 598–610, March 2005.
[13] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", Proc. of ACM MobiCom, Atlanta, GA, USA, September 2002.
[14] Y. Zhang and Y. Fang, "A secure authentication and billing architecture for wireless mesh networks", ACM Wireless Networks, vol. 13, no. 5, pp. 569–582, October 2007.
[15] M. Peirce and D. O'Mahony, "Micropayments for mobile networks", Technical Report of the Department of Computer Science, Trinity College, Dublin, Ireland, 1999.
[16] S. Zhong, J. Chen, and R. Yang, "Sprite: A simple, cheat-proof, credit based system for mobile ad-hoc networks", Proc. of IEEE INFOCOM'03, vol. 3, pp. 1987-1997, San Francisco, CA, USA, March 30-April 3, 2003.
[17] L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A trustful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents", Proc. of ACM MobiCom, San Diego, CA, USA, September 2003.
[18] M. Mahmoud and X. Shen, "FESCIM: Fair, efficient, and secure cooperation incentive mechanism for hybrid ad hoc networks", IEEE Transactions on Mobile Computing (IEEE TMC), In press.
[19] M. E. Mahmoud, and X. Shen, "PIS: A practical incentive system for multi-hop wireless networks", IEEE Trans. on Vehicular Technology, vol. 59, no. 8, pp. 4012-4025, 2010.
[20] M. Mahmoud and X. Shen, "ESIP: Secure incentive protocol with limited use of public-key cryptography for multi-hop wireless networks", IEEE Transactions on Mobile Computing (IEEE TMC), vol. 10, no. 7, pp. 997-1010, July 2011.
[21] M. Mahmoud and X. Shen, "Stimulating cooperation in multi-hop wireless networks using cheating detection system", Proc. IEEE INFOCOM'10, San Diego, California, USA, March 14-19, 2010.
[22] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad-hoc networks", Techical Report, Computer Science Department, Stanford University, CA, USA, July 2003.
[23] S. Buchegger and J. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes – fairness in distributed ad hoc networks", Proc. of IEEE/ACM MOBIHOC, pp. 226-236, Switzerland, June 9-11, 2002.
[24] P. Michiardi and R. Molva, "CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", Proc. of IFIP CMS'02, pp. 107-121, Portoroz, Slovenia, September 26-27, 2002.
[25] Q. He, D. Wu, and P. Khosla, "A secure incentive architecture for ad-hoc networks", Wireless Communications and Mobile Computing, vol. 6, no. 3, pp. 333-346, May 2006.
[26] K. Liu, J. Deng, and K. Balakrishnan. "An acknowledgement-based approach for the detection of routing misbehavior in MANETs," IEEE Transaction on Mobile Computing, vol. 6, no. 5, May 2007.
[27] F. Milan, J. Jaramillo, and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes", Proc. of workshop on Game Theory for Communications and Networks, Pisa, Italy, October 14, 2006.
[28] L. Feeney, "An energy-consumption model for performance analysis of routing protocols for mobile ad hoc networks", Mobile Networks and Applications, vol. 3, no. 6, pp. 239–249, 2001.
[29] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks", Mobile Computing, Chapter 5, Kluwer Academic Publishers, pp. 153-181, 1996.
[30] H. Pagnia and F. Gartner, "On the impossibility of fair exchange without a trusted third party", Technical Report TUD-BS-1999-02, Darmstadt University of Technology, March 1999.
[31] T. Rabin and M. Ben-Or, "Verifiable secret sharing and multiparty protocols with honest majority", Proc. of ACM symposium on Theory of Computing, pp. 73–85, Seattle, Washington, United States, 1989.
[32] C. Cachin, K. Kursawe, A. Lysyanskaya, and R. Strobl, "Asynchronous verifiable secret sharing and proactive cryptosystems", Proc. ACM Conference on Computer and Communications Security, CCS02, pp. 88-97, 2002.
[33] J. Yoon, M. Liu, and B. Nobles, "Sound mobility models", Proc. of ACM MobiCom, San Diego, CA, USA, September 2003.
[34] S. Even, O. Goldreich, and S. Micali, "On-line/off-line digital signatures", Advances in Cryptology--Crypto '89, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 435, pp. 263-277, 1990.
[35] O. Nibouche, M. Nibouche, A. Bouridane, and A. Belatreche, "Fast architectures for FPGA-based implementation of RSA encryption algorithm", Proc. of IEEE Field-Programmable Technology conference, Brisbane, Australia, December 2004.
[36] B. Wu, J. Chen, J. Wu, and M. Cardei, "A survey of attacks and countermeasures in mobile ad hoc networks", Wireless Network Security, Springer, Network Theory and Applications, vol. 17, pp 103-135, 2007.
[37] A. Menzies, P. Oorschot, and S. Vanstone, "Handbook of applied cryptography", CRC Press, http://www.cacr.math.uwaterloo.ca/hac, Boca Raton, Fla., 1996.
[38] NIST, "Digital Hash Standard", Federal information processing standards publication 180-1, April 1995.

Mohamed Elsalih Mahmoud received the B.Sc. and M.Sc. degrees (with honors) in electrical communications engineering from Banha University, Cairo, Egypt, in 1998 and 2003, respectively. He received PhD degree from the University of Waterloo, Department of Electrical and Computer Engineering, in 2011. He is currently post doctoral fellow with the Centre for Wireless Communications, Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada. He is also currently a member of the Broadband Communications Research Group, University of Waterloo. His research interests include wireless network security, privacy, anonymous and secure routing protocols, trust and reputation systems, cooperation incentive mechanisms, and cryptography. He received the Best Paper award from the IEEE International Conference on Communications, Dresden, Germany, 14-18 June 2009. This award is one of the 14 awards among 1,046 papers presented and more than 3,000 total paper submissions and is the unique award for the Communication and Information Systems Security Symposium. He is the first author of more than 13 papers in major IEEE conferences and journals. He also served as a technical program committee member for the Ad Hoc and Sensor Networks track and the Mobile Applications and Services track at the IEEE Vehicular Technology Conference, which was held in Ottawa, Ontario, Canada, 6-9 September 2010.

Xuemin (Sherman) Shen received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 500 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen served as the Technical Program Committee Chair for IEEE VTC'10, the Symposia Chair for IEEE ICC'10, the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also served as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; Computer Networks; and ACM/Wireless Networks, etc., and the Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, an IEEE Fellow, an Engineering Institute of Canada fellow, and a Distinguished Lecturer of IEEE Vehicular Technology Society and Communications Society.