Journal of information and
communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 10(2): 141-148, Jun. 2012 Regular Paper

A Simple but Efficient Scheme for Reliable Connectivity and High Performance in Ad-hoc Wireless Networks

Sungwoo Tak, ***Member, KIICE***

School of Computer Science and Engineering, Pusan National University, Busan 609-735, Korea

Abstract

This paper presents a simple but efficient scheme incorporating a reputation-based approach and a cross-layer approach, called the SIM scheme, for maintaining reliable connectivity and high performance in ad-hoc wireless networks. The SIM scheme incorporates the following two things: an ad-hoc routing scheme with a reputation-based approach exploiting the game theory concept based on an evolutionarily stable strategy, and a cross-layer approach between the network layer and the transport layer employing a reputation-based approach.

Index Terms: Reliable connectivity, Ad-hoc wireless networks, High performance, Trust-based ad-hoc routing

I. INTRODUCTION

In traditional ad-hoc routing protocols, dynamic source routing (DSR) [1] and ad-hoc on demand distance vector (AODV) [2], mobile nodes need to fully cooperate with other mobile nodes as a function of routing and forwarding packets. Unfortunately, when some mobile nodes in ad-hoc wireless networks become selfish nodes to save power, network throughput is dramatically decreased. Additionally, transport protocols may perform poorly due to their inability to distinguish packet losses caused by network congestion from those attributed to intended packet drops by selfish nodes. In this paper, we consider a reputation scheme exploiting the game theory concept based on an evolutionarily stable strategy, called the SIM scheme (a “SIMple” but efficient scheme incorporating a reputation-based approach and a cross-layer approach). Mobile nodes exploiting the SIM scheme monitor and rate the behavior of other mobile nodes in routing and forwarding packets in order to cope with selfish nodes in ad-hoc wireless networks.

Several trust-based approaches have been proposed to reduce the impact of selfish nodes in various networks [3-8]. In particular, the reputation-based cooperation mechanisms presented in [3-5] exploit the reputation evaluation of the mobile nodes derived from the trust model to decide which of them to punish. Additionally, game theory [9] provides us with a method for analyzing an ad-hoc wireless network where selfish and cooperative mobile nodes coexist. In game theory, the best action for each individual decision maker can be found. The game whose objective goal is to isolate selfish mobile nodes belongs to a repeated noncooperation game, where each mobile node takes selfishness into account. The trust-based approach presented in [10] evaluates mobile nodes’ behavior in terms of a non-cooperative game. The packet forward strategy presented in [10] is that each mobile node chooses the action that maximizes its payoff and adjusts the packet forward strategy through the genetic algorithm. However, the genetic

Received 02 April 2012, **Revised** 03 May 2012, **Accepted** 09 May 2012
***Corresponding Author** E-mail: swtak@pnu.edu

Open Access http://dx.doi.org/10.6109/jicce.2012.10.2.141 print ISSN:2234-8255 online ISSN:2234-8883

algorithm has a heavy computational burden. The work addressed in [11] models an ad-hoc network by a cooperative game, where a group of mobile nodes interacts in order to provide packet routing and forwarding services. In the cooperative game, strategies are negotiated and agreed among all the mobile nodes to form a coalition, set up a routing path, and forward packets over the routing path. Consequently, all mobile nodes in the cooperative game are required to negotiate and adopt the agreed strategy but do not take account of misbehaving node issues including no forwarding, free riding, and false feedback.

The SIM scheme proposed in this paper considers three performance deterioration factors in ad-hoc wireless networks, which are no forwarding, free riding, and false feedback, caused by selfish nodes in ad-hoc wireless networks. The performance degradation by no forwarding is that intermediate mobile nodes between source and destination mobile nodes do not forward the received packet to the next hop but drop it. Since this problem has occurred at intermediate mobile nodes, the source node cannot directly detect whether a mobile node is a selfish node or not. The performance degradation by free riding results from free riders, which take advantage of ad-hoc networks without contributing to them. The performance degradation by false feedback results from liars in ad-hoc wireless networks. Liars respond to a successful transaction with a bad reputation or a misbehaving transaction with a good reputation.

In previous research work, the collaborative reputation mechanism [3] was proposed as a reputation technique in order to enforce cooperation among mobile nodes and to prevent passive denial of service attacks due to node selfishness. The cooperation mechanism of mobile nodes presented in [4] employs a reputation system in order to isolate selfish nodes. The mechanism presented in [3] does not consider a liar that generates false feedback to be a major weakness. The approach presented in [4] only detects a liar by the timeout and revocation of reputation values; therefore, it is not robust to collaborative attacks such as a false feedback problem. The reputation scheme presented in [5] assumes that mobile nodes do not lie when sharing their network observations with other mobile nodes and it ignores possible mobile node collusion when aggregating the reputation information from other mobile nodes.

In this paper, the proposed SIM scheme intends to cope with three misbehaviors of selfish nodes - no forwarding, free riding, and false feedback - through a reputation-based approach exploiting a game theory concept based on an evolutionarily stable strategy. Consequently, the SIM scheme leads to maintaining reliable connectivity and high performance in ad-hoc wireless networks. The SIM scheme also attempts to take advantage of a cross-layer approach, where the reputation knowledge dealt with in the network layer is shared with the transport layer. Such a cross-layer approach is useful for improving the efficiency of end-to-end communication performance among mobile nodes in ad-hoc wireless networks. Therefore, the proposed SIM scheme exploits a cross-layer approach for high network performance by interacting with the network layer and the TCP running on the transport layer. This paper is organized as follows. Section II presents the SIM scheme. In Section III, the SIM scheme is evaluated. Section IV concludes this paper.

II. DESIGN OF THE SIM SCHEME

A. Evolutionarily Stable Strategy

The idea of an evolutionarily stable strategy addressed by [12, 13] is that conflict situations will often arise because individual members of many different species have similar needs, and resources are limited. It is especially applicable to the study of selfish nodes in ad-hoc wireless networks. In such a conflict situation, there are several different behavior strategies that an individual mobile node might follow. To resolve a conflict situation, we exploit a game-theoretic model. According to the selfish gene model presented in [12], a pure strategy is an *evolutionarily stable strategy* if the diagonal entry for the pure strategy is the largest entry in the column of the payoff matrix table (e.g., mobile node MN_1's self-defense strategy to mobile node MN_2's self-defense strategy shown in Table 3), since the pure strategy is the best strategy to play when almost every participant is playing the pure strategy.

Mobile nodes of ad-hoc wireless networks will engage in repeated random conflicts over packet transmission to the destination node and packet forwarding to the next hop. In the simple evolutionarily stable strategy model, each conflict is between two kinds of nodes, selfish and virtuous nodes in ad-hoc wireless networks. Mobile nodes are typically constrained by power and computing resources. Thus, a selfish node is not willing to use its computing and energy resources to forward packets that are not directly beneficial to it even though it expects virtuous nodes to forward packets on its behalf. A selfish node uses the network but does not cooperate, saving battery life for its own communications. In this game, the winner who successfully transmits a packet to the destination will get 10 points for taking advantage of the network while the loser who fails to transmit a packet to the destination will get -20 points for being injured calculated as 2 (for power consumption) times -10 (for a packet loss). If both relay nodes adopt the selfish behaving strategy during random periods, they will contend until one mobile node finally takes advantage of the network and the other mobile node is injured. If a selfish node meets a virtuous node, the selfish node will take advantage of the network without sacrificing its battery power and there will be no injury. If two virtuous nodes meet, there will be no injury but both will get -2 points owing to power consumption, waiting for a packet to be processed and delivered.

Table 1. Payoff matrix including selfish and virtuous nodes

MN_1	MN_2	
	Selfish node	Virtuous node
Selfish node	(-5, -5)	(10, 0)
Virtuous node	(0, 10)	(3, 3)
Largest payoff in the column entry from the perspective of MN_1	0	10
Remark	No evolutionarily stable strategy	

Table 1 shows the payoff matrix of the evolutionarily stable strategy based on the game model where there are two players, mobile node MN_1 and mobile node MN_2. Each mobile node has two strategies, i.e. the mobile nodes will decide whether to become a selfish node or a virtuous node. If both mobile nodes pursue the selfish node strategy during random periods, one of two mobile nodes will be a winner and the other will be a loser. Consequently the payoffs are -5 points Q. If both mobile nodes play the virtuous node strategy, one of two mobile nodes can be a winner but there is no loser. Consequently, the payoffs are 3 points $(= \frac{1}{2} \times 10 - 2)$. In Table 1, a population of selfish nodes is not evolutionarily stable because virtuous nodes would be advantages, wining an average of 0 points per encounter compared to an average of -5 points for selfish nodes. Similarly, a population of virtuous nodes is not an evolutionarily stable strategy. A small group of selfish nodes would decrease the population size of virtuous nodes. In Table 1, a mixed strategy consisting of the probability $\frac{7}{12}$ of being a selfish node and the probability $\frac{5}{12}$ of being virtuous node is an evolutionarily stable strategy for this game. The strategy leading to this outcome is the best response to each other. Mobile node MN_1 and mobile node MN_2 are guaranteed to do no worse than this value. At this point, each mobile node does not need to be a pure selfish node or a pure virtuous node.

We now introduce a new possible node type, a cheating node. The cheating node first pretends to be a selfish node and continues to be a selfish node if its opponent remains a virtuous node. If its opponent becomes a selfish node, it stops being a selfish node. Table 2 shows the payoff matrix including the cheating node where there are two players, mobile node MN_1 and mobile node MN_2. If both mobile nodes adopt the cheating node strategy, one of the two mobile nodes can be a winner as a selfish node if the other plays a virtuous node. Consequently, the payoffs are 5 points $(= \frac{1}{2} \times 10)$.

Table 2. Payoff matrix including a cheating node

MN_1	MN_2		
	Selfish node	Virtuous node	Cheating node
Selfish node	(-5, -5)	(10, 0)	(10, 0)
Virtuous node	(0, 10)	(3, 3)	(0, 10)
Cheating node	(0, 10)	(10, 0)	(5, 5)
Largest payoff in the column entry from the perspective of MN_1	0	10	10
Remark	No evolutionarily stable strategy		

In Table 2, the cheating node dominates the virtuous node strategy. Thus, Table 2 reduces to only selfish and cheating nodes, and the mixed strategy consisting of the probability $\frac{1}{2}$ of being a selfish node and the probability $\frac{1}{2}$ of being cheating node is the best response of the nodes to each other for this game. Selfish and cheating nodes behave selfishly, looking out for only their own node's interest. Namely, selfish and cheating nodes behave maliciously, seeking to ruin network performance. In Table 2, a great deal of greedy and cowardly behavior may occur in ad-hoc wireless networks. To cope with the cheating node, we introduce an additional node type, a self-defense node. The self-defense node first behaves like a virtuous node. However, if the self-defense node is attacked by a selfish node, it changes into a selfish node with reasonable force.

Table 3 shows the payoff matrix including the self-defense node. In Table 3, the pure self-defense strategy is an evolutionarily stable strategy because the diagonal entry for the pure strategy, the self-defense strategy of both MN_1 and MN_2, is the largest entry in the column of Table 3. In particular, the self-defense node will always win the game against the cheating node without conflict. In a population of self-defense nodes, we would see no real conflict. The analysis of Table 3 shows that this kind of peaceful equilibrium can be maintained by reasonable force in ad-hoc wireless networks.

Table 3. Payoff matrix including a self-defense node

MN_1	MN_2			
	Selfish node	Virtuous node	Cheating node	**Self-defense node**
Selfish node	(-5, -5)	(10, 0)	(10, 0)	(-5, -5)
Virtuous node	(0, 10)	(3, 3)	(0, 10)	(3, 3)
Cheating node	(0, 10)	(10, 0)	(5, 5)	(0, 10)
Self-defense node	(-5, -5)	(3, 3)	(10, 0)	**(3, 3)**
Largest payoff in the column entry from the persepctive of MN_1	0	10	10	**3**
Remark	MN_1′s self-defense strategy to MN_2′s self-defense strategy is an evolutionarily stable strategy			

B. Reputation-based Approach

In the previous section, the problem of routing in an ad-hoc wireless network is well explained by a game theory concept based on the evolutionarily stable strategy. Traditional ad-hoc wireless routing protocols are composed of routing and forwarding phases. Unfortunately, some selfish nodes might intend not to forward packets in order to save resources for their own use. To detect selfish nodes, an ad-hoc routing protocol enables a mobile node to determine the trustworthiness of other mobile nodes with respect to reliable packet delivery by combining trustworthiness information directly obtained from its neighbor mobile nodes and trustworthiness information indirectly obtained from other mobile nodes. Hence, in ad-hoc wireless networks where individual mobile nodes are expected to perform services on behalf of other mobile nodes, the question of trust and reputation management becomes important.

In the analysis results from section II-A, the pure self-defense node strategy is an evolutionarily stable strategy. We apply the concept of the self-defense node strategy to the SIM scheme proposed in this paper. The basic idea of the SIM scheme is for each mobile node to assign a reputation value to all other mobile nodes with which it comes into contact in an ad-hoc wireless network. As a mobile node's perceived reputation decreases, its neighbors may refuse to perform service for it as a self-defense strategy, leading to its gradual exclusion from the network. The proposed SIM scheme evaluates the trust between two neighbor nodes from first-hand observation data. After each mobile node forwards a packet to the next hop node, it monitors and rates the behavior of the next hop node in forwarding, and responds according to its opinion about the next hop node. The opinion that a mobile node has of another is called reputation. Additionally, the SIM scheme uses reputation measurement in the routing phase to detour selfish nodes and encourage the cooperation of mobile nodes. A routing path between a source node and its destination node is found via the SIM scheme exploiting reputation management. The reputation management of the SIM scheme technically deals with how and what evidence is gathered for the trustworthiness of each mobile node, how trustworthiness is calculated, and how trust values are updated to maintain a reliable ad-hoc wireless network.

We first describe the reputation management of the SIM scheme used in the network layer. The mobile node MN_j is said to be a neighbor of mobile node MN_i if MN_i can hear the packet transmission of MN_j on the wireless interface, where i and j represent positive integers. *Reputation* (MN_i, MN_j, T_k) denotes the reputation value of MN_j evaluated by MN_i at transaction T_k, where k is a nonnegative integer. For example, if mobile node MN_2, a neighbor of mobile node MN_1, is cooperative with MN_1 at the k-th transaction T_k, MN_1 considers the reputation of MN_2 to be good and assigns the reputation value of MN_2, *Reputation* (MN_1, MN_2, T_k), to 1 as a good reputation. Otherwise, *Reputation* (MN_1, MN_2, T_k) = -1 as a bad reputation. *Virtuous* (MN_i, MN_j, T_k) and *Selfish* (MN_i, MN_j, T_k) represent the number of good reputations and bad reputations of MN_j's behaviors, which are evaluated by MN_i at transaction T_k.

The confidence represents the long-term trustworthiness of each mobile node. *Confidence* (MN_i, MN_j, T_k) denotes the confidence value of mobile node MN_j evaluated by mobile node MN_i at transaction T_k. We exploit the value of trustworthiness as the measurement for selecting an optimal routing path and the value of confidence as the measurement for detecting a liar. The confidence value of mobile node MN_j evaluated by mobile node MN_i is derived by Eq. (1). The confidence in other mobile nodes is evaluated by considering trustworthiness values, *Virtuous* (MN_i, MN_j, T_k) and *Selfish* (MN_i, MN_j, T_k), which result from all of the transactions up to the present transaction T_k. Thus a liar can be isolated from the network even if a selfish node is disguised as a good-behaving mobile node and tries to participate in the network.

$$\textsc{Confidence}\left(MN_i, MN_j, T_k\right) = \frac{\{\sum_{x=0}^{k} \textsc{Virtuous}\left(MN_i, MN_j, T_x\right) - \left|\sum_{x=0}^{k} \textsc{Selfish}\left(MN_i, MN_j, T_x\right)\right|\}}{\{\sum_{x=0}^{k} \textsc{Virtuous}\left(MN_i, \mathrm{MN}_j, T_x\right) + \left|\sum_{x=0}^{k} \textsc{Selfish}\left(MN_i, MN_j, T_x\right)\right|\}} \qquad (1)$$

We now describe the procedure of deriving *Virtuous* (MN_i, MN_j, T_k) and *Selfish* (MN_i, MN_j, T_k) values described in Eq. (1), which are the number of accumulated good and bad reputations of MN_j's behavior at transaction T_k. Let us assume that there is an end-to-end forwarding path, MN_1 - MN_2 - MN_3 - MN_4, between source MN_1 and destination MN_4. We assume that mobile node MN_1 forwards a packet to the next hop node MN_2 at transaction T_k. However, MN_2 does not forward the packet transmitted from MN_1 due to MN_2's selfishness. Then MN_1 thinks of MN_2 as a selfish node and sets the value of *REPUTATION* (MN_1, MN_2, T_k) = -1. MN_1 evaluates and updates *SELFISH* (MN_1, MN_2, T_k) through Eq. (2).

$$\textsc{Selfish}\ (MN_i, MN_j, T_k) = \sum_{y \leftarrow \text{neighborhood}(MN_i)} \textsc{Confidence}\ (MN_i, MN_y, T_k) \times \textsc{Selfish}\ (MN_y, MN_j, T_k) + \textsc{Weight} \times \textsc{Reputation}(MN_i, MN_j, T_k), \text{where } \textsc{Weight} = 1 + \alpha \text{ if } \textsc{Reputation}(MN_i, MN_j, T_{k-1}) = -1, \text{otherwise } \textsc{Weight} = 1 \quad (2)$$

In Eq. (2), if the reputation values of the previous transaction ($T_{k\text{-}1}$) and present transaction (T_k) are equal to each other, the reputation value is weighted as (1 + α) times. In case mobile node MN_2 continues to drop packets, its reputation value begins to degenerate by the outcome of Eq. (2). The value of α is set to 0.2 in experiments carried out in this paper.

$$\textsc{Virtuous}\ (MN_i, MN_j, T_k) = \sum_{y \leftarrow \text{neighborhood}(MN_i)} \textsc{Confidence}\ (MN_i, MN_y, T_k) \times \textsc{Virtuous}\ (MN_y, MN_j, T_k) + \textsc{Weight} \times \textsc{Reputation}(MN_i, MN_j, T_k), \text{where } \textsc{Weight} = 1 + \alpha \text{ if } \textsc{Reputation}(MN_i, MN_j, T_{k-1}) = 1, \text{otherwise } \textsc{Weight} = 1 \quad (3)$$

If mobile node MN_2 forwards a packet transmitted from mobile node MN_1, MN_1 thinks of MN_2 as a virtuous node and set the value of *REPUTATION* (MN_1, MN_2, T_k) = 1. The MN_1 evaluates and updates *VIRTUOUS* (MN_1, MN_2, T_k) through Eq. (3), in which we substitute *SELFISH* (MN_i, MN_j, T_k) with *VIRTUOUS* (MN_i, MN_j, T_k) in Eq. (2). In case MN_2 successfully continues to forward packets, Eq. (3) exploiting *VIRTUOUS* (MN_1, MN_2, T_k) makes mobile node MN_2 more trustworthy. When there exist liars who respond to a successful transaction with a bad reputation or a misbehaved transaction with a good reputation, Eq. (3) is weighted by *CONFIDENCE* (MN_1, MN_y, T_k), where y denotes a set of neighbors of mobile node MN_1.

In Eq. (4), *TRUST* (MN_i, MN_j, T_k) denotes the trustworthiness value of mobile node MN_j evaluated by mobile node MN_i at transaction T_k. This represents the short-term measurement for each mobile node to calculate how cooperative its neighbors have been most recently.

$$\textsc{Trust}\ (MN_i, MN_j, T_k) = \textsc{Load}\ (MN_i, MN_j, T_k) \times \textsc{Confidence}\ (MN_i, MN_j, T_k), \quad (4)$$

$$\text{where } k = \text{uniform distribution over recent } (k - 60, k - 1) \text{ transctions up to transaction k}$$

$$\text{and } \textsc{Load}\ (MN_i, MN_j, T_k) = 1 - \frac{\sum_y \textsc{Virtuous}\ (MN_y, MN_j, T_k)}{\sum_y \sum_z \textsc{Virtuous}\ (MN_y, MN_z, T_k)}$$

$$\text{with } y \text{ } and \text{ } z \leftarrow \text{neighborhood}(MN_i)$$

The value of *TRUST* (MN_i, MN_j, T_k) is used to measure the trustworthiness of several routing path candidates between two end mobile nodes. Then, we set up the routing path with the best trustworthiness product value (primary criteria) and minimum hops (secondary criteria). For example, as described earlier, the trustworthiness product value of an end-to-end delivery path between MN_1 and MN_4 (i.e., MN_1 - MN_2 - MN_3 - MN_4) at transaction T_k is equal to *TRUST* (MN_1, MN_2, T_k) × *TRUST* (MN_2, MN_3, T_k) × *TRUST* (MN_3, MN_4, T_k). The experimental default value of the short-term transaction period exploited in the experiments is uniformly distributed over the recent (k - 60, k - 1) transactions up to transaction k. Since trustworthiness is determined from the result of transactions during the short-term transaction period, it figures how well each mobile node has been cooperating with its neighbors most recently. Thus, a selfish node has a chance that it will recover from the status of selfish node in the short-term transaction period and then it is allowed to transmit packets over the network. If the selfish node continuously resists cooperating with other mobile nodes, the amount of time in which the mobile node is isolated by its neighbors is increased exponentially.

After transaction T_k is finished, mobile node MN_1 calculates the trustworthiness of mobile node MN_2, *TRUST* (MN_i, MN_j, T_k) using equation (4) where i = 1 and j = 2. There is a possibility that a mobile node with the highest reputation value is selected as one of the relay mobile nodes; consequently, network traffic continuously flows into the mobile node, and thus its battery power will be consumed quickly. To resolve this problem, *TRUST* (MN_1, MN_2, T_k) is weighted by *LOAD* (MN_1, MN_2, T_k). The *LOAD* (MN_1, MN_2, T_k) implies the complement of a share of mobile node MN_2's good reputation values distributed over MN_1's neighbors.

C. Cross-layer Approach

Generally, ad-hoc wireless networks consider the node mobility problem. However, due to high error rates and low bandwidth in the wireless domain, there obviously needs to be a higher layer abstraction that would perform three control mechanisms: error control, congestion control, and flow control.

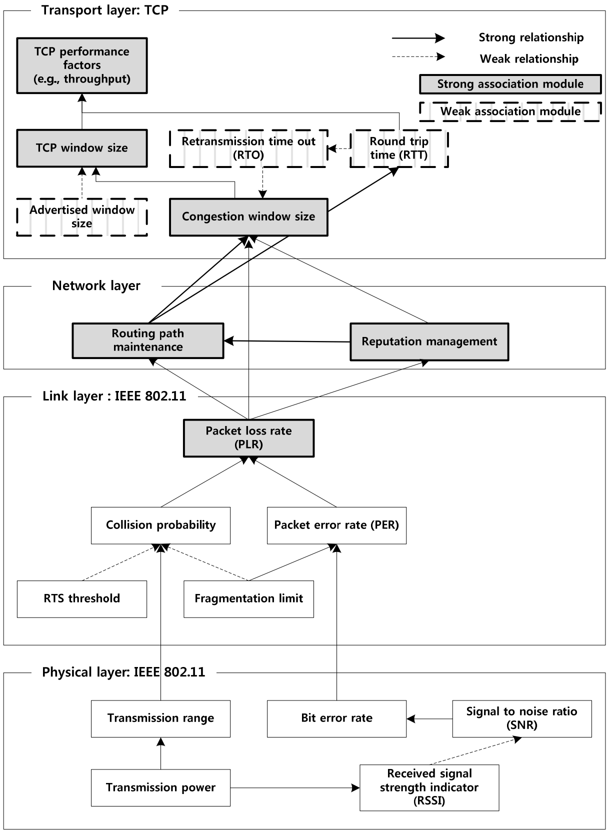

Fig. 1. Interdependencies in communication layers.

The classical transport protocol, TCP, has been widely exploited to guarantee in-order and reliable delivery in wired networks. TCP is a reliable, end-to-end, and connection-oriented transport layer protocol that provides a byte-stream-based service. Since the transition to the wireless domain should be compatible with the existing infrastructure, there is a need for modifications of the TCP protocol. This is the correct approach, rather than resorting to a completely new set of protocols. We first analyze interdependencies among communications layers, which are the IEEE802.11-based physical and link layers, the network layer, and the TCP-based transport layer to determine the correct approach. As illustrated in Fig. 1, the TCP in ad-hoc wireless networks performs poorly due to its inability to distinguish packet losses caused by network congestion from those attributed to packet drops intended by selfish nodes.

To resolve this problem, we propose two feasible but independent TCP approaches exploiting the SIM scheme. One is that we apply the concept of trustworthiness of a forwarding path to the TCP fast recovery technique. The other approach is that we apply the concept of trustworthiness of a forwarding path to the TCP rate adaptive congestion control. In the TCP rate adaptive congestion control exploiting the trustworthiness value described in section II-B, a mobile node controls the TCP sending rate based on the trustworthiness value of a forwarding path before many packets are dropped by selfish nodes. For example, the trustworthiness value of a forwarding path at transaction *k* is represented by the TRUSTWORTHINESS PATH VALUE. In the case of the TRUSTWORTHINESS PATH VALUE of a path between MN_1 and MN_4, consisting of MN_1 - MN_2 - MN_3 - MN_4 at transaction T_k, it is equal to the product of the TRUST (MN_1, MN_2, T_k), TRUST (MN_2, MN_3, T_k), and TRUST (MN_3, MN_4, T_k) values. The TCP fast recovery with the SIM scheme is carried out as follows: For each additional duplicate *ACK* received, the TCP congestion window denoted by the CONGESTION WINDOW is decreased as follows:

$$\Delta\textsc{Congestion Window} = \left(\textsc{Congestion Window} - \textsc{Slow Start Threshold}\right) \times \left(1 - \textsc{Trustworthiness Path Value}\right) \times \frac{\textsc{Maximum Segment Size}}{2} \qquad (5)$$

Eq. (5) implies an implicit notification of packet drops by a selfish node over the end-to-end forwarding path. Note that the TCP sets the value of the SLOW START THRESHOLD to half of the current CONGESTION WINDOW value when the third duplicate ACK is received [14]. In the TCP rate adaptive congestion control exploiting the reputation value, the TCP congestion window is decreased as follows:

$$\textsc{Congestion Window} = \frac{1}{\textsc{Round Trip Time}} - \frac{\textsc{Congestion Window}}{2} \times \textsc{PacketLossRate}, \qquad (6)$$

$$\text{Where } \textsc{PacketLossRate} = \text{TCP } \textsc{Throughput} \times \left(1 - \textsc{Trustworthiness Path Value}\right)$$

The first term in Eq. (6) represents the additive increase part of the TCP, where the TCP congestion window size will be increased by one per the round trip time. The second term in Eq. (6) represents the multiplicative decrease part. When a packet drop occurs, it halves the TCP congestion window size at the instant of the packet loss as a multiplicative decrease. We assume that packet drops will be caused by selfish nodes not network congestion. The packet loss rate is affected by TCP throughput and TRUSTWORTHINESS PATH VALUE. The value of the TRUSTWORTHINESS PATH VALUE is determined by the trustworthiness value of a forwarding path.

III. EXPERIMENTS

We evaluated the performance verification of the SIM scheme on the NS-2 simulator. In the simulation, we deployed 50 mobile nodes randomly in a rectangular field (1,000 × 500 m). Each mobile node has an omni-directional antenna with a range of 100 m, and the random-way-point mobility model [15] is used to simulate the movements of the mobile nodes. Mobile nodes have pause times at either 10 or 5 seconds. The movements of the mobile nodes result in disconnecting the established routing paths. We select some nodes to be activated as selfish nodes. The percentage of selfish nodes ranges from 0% to 80%. With a probability of 0.3, they randomly misbehave in one of the following ways: no forwarding, free riding, and false feedback, which are caused by selfish nodes in ad-hoc wireless networks. During the simulation time of 20,000 seconds, a constant bit rate (CBR) of 50 connections was active and each mobile node transmited a 10 Kbps stream of data to its destination node. We ran AODV and DSR protocols with the reputation management of the SIM scheme. Table 4 shows the performance of the proposed SIM scheme.

Table 4. Performance of the SIM scheme according to the percentage of selfish nodes (percentage)

Selfish node distribution	0	20	40	60	80
DSR (packet loss)	14	73.6	79.8	90.6	99
AODV (packet loss)	13.8	70.4	79.6	89.6	98.5
DSR with SIM (packet loss)	14	48.5	56.2	68.2%	95.2
AODV with SIM (packet loss)	13.8	40.2	49	59	80.5

DSR: dynamic source routing, AODV: ad-hoc on demand distance vector.

In Table 4, the packet loss ratio increases as the percentage of selfish nodes increases. However, when the reputation management exploited in the SIM scheme is incorporated into each of two routing protocols (AODV and DSR protocols), they achieve a lower packet loss ratio than their original versions. As described in Table 4, the poor performance of the DSR protocol is mainly attributed to aggressive use of caching and the lack of any mechanism for removing stale routes or determining the freshness of routes when multiple choices are available [16]. The connection setup delay of the DSR protocol is higher than the table-driven protocol, the AODV protocol. In order to maintain routes using the AODV protocol, the AODV protocol normally requires that each mobile node periodically transmit a HELLO message with a default rate of once per second. Failure to receive three consecutive HELLO messages from a neighbor is taken as an indication that the link to the neighbor in question is down. In our experimentation, we determine that a link breaks by observing three consecutive HELLO messages.

Table 5. Normalized TCP throughput incorporating the SIM scheme by percentage of selfish nodes

Selfish Node Distribution	0%	20%	40%	60%	80%
TCP	0.42	0.13	0.1	0.045	0.004
TCP fast recovery with SIM	0.42	0.20	0.17	0.1	0.02
TCP rate adaptive congestion control with SIM	0.42	0.3	0.25	0.2	0.09

Table 5 shows the normalized TCP throughput over the ADOV protocol incorporating the SIM scheme. We compare the performance of the original TCP to the performance of the TCP fast recovery with the SIM scheme, and the TCP rate adaptive congestion control with the SIM scheme over varying selfish node proportions. The TCP regards packet drops by selfish nodes as network congestion due to the generic limitations of TCP in ad-hoc wireless network environments. Then the original TCP starts to halve the congestion window to avoid network congestion. In case of the TCP fast recovery with the SIM scheme, it can detect packet drops by selfish nodes implicitly and recover the TCP congestion window quickly up to the congestion window size just before packets drop. In case of the TCP rate adaptive congestion control with the SIM scheme, it controls its TCP sending rate in order to dynamically adapt the transient status of networks and minimize the number of packets dropped by selfish nodes. This does not result in the unnecessary decrease of the congestion window size. The TCP rate adaptive congestion control with the SIM scheme achieves better performance than the original TCP and the TCP fast recovery with the SIM scheme.

IV. CONCLUSIONS

We propose a SIM scheme for reliable connectivity and high performance in ad-hoc wireless networks. The SIM scheme incorporates a reputation-based approach exploiting a game theory concept based on an evolutionarily stable strategy, and a cross-layer approach exploiting the proposed reputation management. We measure the performance of the SIM scheme and experimental outcomes show that the SIM scheme achieves efficient performance in terms of a low packet loss ratio and high network throughput.

REFERENCES

[1] D. Johnson, Y. Hu, and D. Maltz, “The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4,” The Internet Engineering Task Force, Fremont, CA, *RFC 4728*, 2007.

[2] C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc on-demand distance vector (AODV) routing,” The Internet Engineering Task Force, Fremont, CA, *RFC 3561*, 2003.

[3] S. Buchegger and J. de Boudec, “Performance analysis of the CONFIDANT protocol,” *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking & Computing*, Lausanne, Switzerland, pp. 226-236, 2002.

[4] P. Michiardi and R. Mova, “Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” *Proceedings of the 6th Joint Working Conference on Communications and Multimedia Security*, Portoroz, Slovenia, pp. 107-121, 2002.

[5] Q. He, D. Wu, and P. Khosla, “SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks,” *Proceedings of IEEE Wireless Communications and Networking Conference*, Atlanta, GA, pp. 825-830, 2004.

[6] F. Almenarez, A. Marin, D. Diaz, and J. Sanchez, “Developing a model for trust management in pervasive devices,” *Proceedings of the 4th IEEE International Conference on Pervasive Computing and Communications Workshop*, Pisa, Italy, pp. 1-5, 2006.

[7] A. Boukerch, L. Xu, and K. El-Khatib, “Trust-based security for wireless ad hoc and sensor networks,” *Computer Communications*, vol. 30, no. 11-12, pp. 2413-2427, 2007.

[8] A. Ukil, “Secure trust management in distributed computing systems,” *Proceedings of the 6th IEEE International Conference on Electronic Design, Test and Application*, Qeenstwon, New Zealand, pp. 116-121, 2011.

[9] P. K. Dutta, *Strategies and Games: Theory and Practice*, Cambridge, MA: MIT Press, 1999.

[10] M. Seredynski, P. Bouvry, and M. A. Klopotek, “Modelling the evolution of cooperative behavior in ad hoc networks using a game based model,” *Proceedings of IEEE Symposium on Computational Intelligence and Games*, Honolulu, HI, pp. 96-103, 2007.

[11] J. S. Baras and T. Jiang, “Cooperation, trust and games in wireless networks,” in *Advances in Control, Communication Networks, and Transportation Systems, Boston*, MA: Birkhauser, pp. 183-202, 2005.

[12] J. M. Smith and G. R. Price, “The logic of animal conflict,” *Nature*, vol. 246, no. 5427, pp. 15-18, 1973.

[13] P. D. Straffin, *Game Theory and Strategy*, Washington, DC: Mathematical Association of America, 1993.

[14] M. Allman, V. Paxson, and W. Stevens, “TCP congestion control,” The Internet Engineering Task Force, Fremont, CA, *RFC 2581*, 2001.

[15] T. Camp, J. Boleng, and V. Davies, “A survey of mobility models for ad hoc network research,” *Wireless Communications & Mobile Computing*, vol. 2, no. 5, pp. 483-502, 2002.

[16] S. R. Das, C. E. Perkins, and E. M. Royer, “Performance comparison of two on-demand routing protocols for ad hoc networks,” *Proceedings of the 9th Joint Conference of the IEEE Computer and Communications Societies*, Tel Aviv, Israel, pp. 3-12, 2000.

Sungwoo Tak

is an associate professor in the School of Computer Science and Engineering at Pusan National University. He is also a research member at the Research Institute of Computer Information and Communication at Pusan National University. He received a Ph.D. degree in Computer Science from the University of Missouri – Kansas City. His research interests include computer networks, wireless networks, software architecture, WDM optical networks, real-time systems, and network processor design