This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the WCNC 2008 proceedings.

A Novel Fair Incentive Protocol for Mobile Ad Hoc Networks

Rongxing Lu, Xiaodong Lin, Haojin Zhu, Chenxi Zhang, Pin-Han Ho and Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada N2L 3G1
Email: {rxlu, xdlin, h9zhu, pinhan, xshen}@bbcr.uwaterloo.ca, c14zhang@engmail.uwaterloo.ca

***Abstract*—To enhance the overall performance of a mobile ad hoc network (MANET), people have tried to solve the issue of node selfishness, which has sparked a surge of research interests in credit-based incentive protocols. The core idea of credit-based incentive is to provide incentives for selfish nodes to faithfully forward packets in a MANET. Recently, several credit-based incentive protocols have been proposed. However, the fairness issue in those reported credit-based incentive protocols has never been well addressed yet. Without the fairness guarantees, the whole network still cannot reach its optimum cooperative status. Therefore, in this paper, aiming at fairness, we first define the fairness principle for credit-based incentive protocol, and then present a novel fair incentive protocol (FIP) for MANETs.**

***Keywords* — MANET, selfish node, credit-based incentive, fairness.**

I. Introduction

A mobile ad hoc network (MANET) is a self-organizing and rapidly deployable network, which is comprised of many mobile computing devices as communication nodes without any assistance from the fixed infrastructure or prior configuration of the network nodes, as that in the traditional wireless network. Therefore, in recent years, the attractive non-infrastructure nature of MANETs has gained a lot of attention with many research efforts that have been addressed [1], [2]. In general, the applications of MANETs can range from the military scenarios to the civilian applications. In military applications, all mobile nodes belong to the same organization and will cooperate with each other toward a common goal (such as tactical communications in digital battlefields). However, in the civilian environments, the mobile nodes have different owners such that they may not be willing to help the others to forward packets due to various reasons. For example, in order to conserve power and computing resources, a selfish mobile node may be very reluctant in the cooperation that is not directly beneficial to it, which could simply leave a well designed routing protocol useless. Therefore, how to efficiently and effectively resolve this problem of selfishness and create a fair environment in the civilian applications has become an important challenge in MANETs.

In recent years, a lot of researchers have identified the above issue, and many schemes to stimulate the possible selfish nodes for forwarding packets have been proposed [3]–[12]. Basically, these schemes can fall into two categories, namely, reputation-based schemes and credits-based schemes. In the reputation-based schemes [3]–[6], normal mobile nodes collectively identify the selfish nodes, establish a route that can avoid these selfish nodes, and disseminate the bad reputations of these selfish nodes throughout the network. However, as discussed in [11], [12], there are several issues existing in the reputation-based systems. For example, when some selfish nodes are in collusion, it is hard to prevent the propagation of incorrect reputations. The core idea of credit-based schemes is to provide incentives for selfish nodes to faithfully forward packets in a MANET. Specifically, the credit, a virtual currency, is set up in the credit-based schemes. Each node with a credit account will get credits for helping forwarding the other nodes' packets. At the same time, it also uses its credits to pay other nodes for their help. Therefore, the credit-based incentive schemes have received great attention in the civilian scenarios [7]–[12].

By taking credits as virtual currency, the credit-based incentive scheme in MANET is somewhat like an electronic commerce system, which is inevitably subject to the *fairness* issue [13]. However, to the best of our knowledge, all the previously reported credit-based studies have never addressed the *faireness* issue completely. Because a MANET is an open environment, the *fairness* issue could arise in two situations: i) the intermediate nodes may worry that it cannot receive any credit from the source node even after helping the source node forward packets; and ii) The source node may worry that the intermediate nodes keep on being selfish even after paying them the credits. Therefore, a discipline must be defined for both source node and intermediate nodes such that no one can take advantages against the other even if one of them still has a selfish intent.

In this paper, we address the above fairness concern by devising a fair incentive protocol (FIP) for MANETs to deal with the selfish nodes in the civilian application scenarios. Our major contributions are in two folds and are summarized as follows.

- We explicitly define the *fairness* principle in a credit-based incentive protocol in MANETs, and propose a novel fair incentive state transition model for analyzing the status of a MANET. To the best of our knowledge, our work is the first such effort towards the selfish civilian MANETs.
- Secondly, we design a novel fair incentive protocol (FIP) in MANETs based on an efficient and provable secure short signature [14], short verifiably encrypted signature [15], and short aggregate signature [16]. From the analysis, the proposed FIP can achieve fairness such that the whole MANET will reach its optimal operational status.

The rest of this paper is organized as follows. In Section II, we characterize the fair incentive in MANETs. Then, the proposed FIP is presented in Section III, followed by the

1525-3511/08/$25.00

fairness analysis in Section IV. Finally, we draw conclusions and brief our future work in Section V.

II. Characterizing the Fair Incentive in MANETs

In this section, we characterize the fair incentives in MANETs by firstly formulating the network model, the incentive strategy, and then identifying the desired fairness objectives.

A. Network Model

Fig. 1 gives the overall architecture of the system considered in our study, which includes a *Trusted Credit Clearance Service* (TCCS) and a MANET consisting an unconstrained number of mobile nodes $\mathcal{N} = \{N_1, N_2, \cdots, N_n\}$.

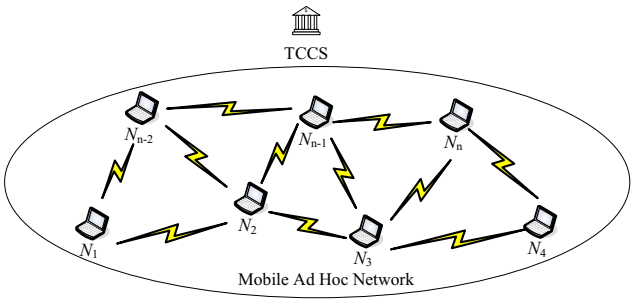

Fig. 1. Network model under consideration

1) TCCS: It is trusted by all entities in the system and maintains all mobile nodes' credit accounts. It performs trusted fair credit clearance when any mobile node requests for.

2) MANET: We consider the MANET in our system as in the civilian scenarios, where the mobile nodes are either normal-behaved or selfish, but never irrationally malicious as that in the military scenarios. Due to the selfishness of some mobile nodes, the MANET cannot be assumed cooperative.

3) Mobile nodes: In the civilian MANET considered in this study, the mobile nodes can be laptop computers, personal digital assistants (PDAs) and hand-held devices whose softwares enable their network roaming capabilities. However, since the typical mobile nodes have some certain constraints such as power shortages and computation resource limitations, the mobile nodes may become selfish and are unwilling to cooperate with others to forward packets, although they could still operate normally in the Route Discovery and the Route Maintenance phases.

B. Incentive Strategy

In order to prevent the overall performance degradation due to the selfish mobile nodes, the credit-based incentive strategy is considered in the system. Like in [7]–[12], the basic strategy is to provide incentives for intermediate nodes to faithfully forward packets. Concretely, the intermediate nodes will get paid for packet forwarding for the other nodes, and will take the same payment mechanism to pay for their packet forwarding requests, by which the overall performance of the MANET can be assured.

To realize the credit-based incentive strategy, the following assumptions are raised.

1) Each mobile node should have a unique nonzero ID, a pair of certificated public and private keys, and can support cryptographic operations.

2) Each mobile node should have a credit account to store its credits, which are used for paying the other nodes' packet forwarding assistance. In general, a mobile node can earn credits in the following two ways: i) purchase credits with real money; and ii) receive credits by forwarding packets for the other peer nodes. Similar to the credit cards in the real life, a mobile node is allowed to request services first and perform the credit clearance operation with the TCCS later on.

3) The TCCS is trusted and has a pair of public and private keys, which fairly performs credit clearance operations for the mobile nodes. (Note that: based on Pagnia and Gartner's proof result in [17], we know it is impossible to realize fairness between two entities while without a trusted third party (TTP). So the TCCS is introduced.)

4) The communication between the mobile nodes is bidirectional, i.e., two nodes within the wireless transmission range may directly communicate with each other based on the popular wireless 802.11 protocol [18]. However, due to the nature of mobility, the wireless channel may be unreliable.

5) A mobile node can report to the TCCS for credit clearance, through a fast and secure channel [11].

C. Fairness Objectives

In a civilian selfish MANET with an incentive strategy, some mobile nodes could still be selfish and cause unfair events while forwarding packets. This happens in the following two situations, which will be considered in this study: i) After the intermediate nodes forward packets for the source node to the destination node, the source node collude with the destination node to deny paying the credits to the intermediate nodes. ii) The intermediate nodes which have obtained the credits from the source nodes are still reluctant to forward packets for the source nodes. Both of the situations result in unfairness and may yield fatal impact on the system cooperation.

In this study, an atomicity principle is defined: "*The intermediate nodes can receive credits if and only if the destination node receives the packets.*", which will serve as the basis in the design of our incentive strategy. According to the atomicity principle, we subtly depict four states as shown in Fig. 2, which demonstrates the relation between the fairness and incentive strategy in the MANET.

STATE 0 has no incentive strategy and fairness issue, where all mobile nodes are selfish and no-cooperate. Thus, the whole network is in degradation.

STATE 1 is fair and the whole network lies in its optimum cooperative status. All the mobile nodes are normal-behaved due to the incentive strategy, and the atomicity principle follows.

STATE 2 is unfair. Although the incentive strategy is injected, the source / destination nodes are still selfish as in case i). Therefore, due to this unfairness, the whole network cannot reach its optimum cooperative status.

STATE 3 is also unfair. The unfair status is due to the selfishness of the intermediate nodes as described in case ii). The whole ad hoc network is in degradation.

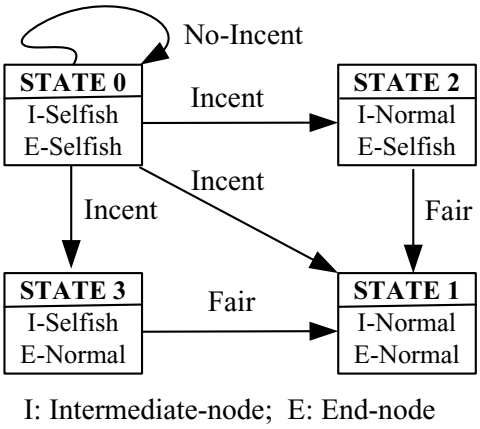

Fig. 2. Fair incentive state transition model for ad hoc networks

Based on the above state definition, the fairness objectives in this work is to provide efficient fairness strategy to push unfair STATE 2 and STATE 3 to the optimum cooperative STATE 1 status. To the best of our knowledge, no previous work has worked out a good solution for this purpose. Our fair incentive protocol (FIP), which is believed the first effort on successfully tackling this issue for MANETs, will be presented in the following section.

III. Proposed FIP Protocol

A. Pairing Technique

Let $\mathbb{G}$ be an additive cyclic group of prime order q, and $\mathbb{G}_T$ be a multiplicative cyclic group of the same order. Assume that the discrete logarithm (DL) problem is hard in both $\mathbb{G}$ and $\mathbb{G}_T$. An admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ between these two groups satisfies i) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}$ and all $a, b \in \mathbb{Z}_q^*$, ii) Non-degenerate: $e(P, Q) \neq 1$ and iii) Computable. Typically, we can make the bilinear map using modified Weil or Tate pairing [19].

Definition 1: A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input and outputs a 5-tuple $(q, P, \mathbb{G}, \mathbb{G}_T, e)$ where q is a k-bit prime number, $(\mathbb{G}, +)$ and $(\mathbb{G}_T, \times)$ are two groups with order q, $P \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is an admissible bilinear map.

B. Design of Fair Incentive Protocol

This subsection describes the design of our FIP. The FIP will be presented by dividing it into the following four parts: System setting, Routing setting, Fair incentive packet forwarding, and Trusted fair credit clearance.

1) System setting: For clear and easy presentation, we assume that all mobile nodes and TCCS are using the same suite of system parameters. Given the security parameter k, the bilinear parameter $(q, P, \mathbb{G}, \mathbb{G}_T, e)$ are first generated by running $\mathcal{G}en(k)$. Then, three hash functions H, h, f and symmetric encryption algorithm $\mathcal{E}()$ are chosen. In the end, the system parameters $\mathsf{params} = (q, P, \mathbb{G}, \mathbb{G}_T, e, H, h, f, \mathcal{E})$ are published. TCCS chooses a random number $x_T \in \mathbb{Z}_q^*$ as its private key sk_T and computes the public key pk_T as $Y_T = x_T P$. Similarly, each mobile node $N_i \in \mathcal{N}$ also chooses a random number $x_i \in \mathbb{Z}_q^*$ as its private key sk_i and computes the public key pk_i as $Y_i = x_i P$. Note that, all public keys should be certified by public key certificates issued by *certificate authority* (CA).

2) Routing setting: Ad hoc On-demand Distance Vector (AODV) is a method of routing messages between mobile nodes in MANETs, which enables multi-hop communication and packet relaying. AODV does this by discovering the routes, which should be loopless and shortest [20]. In the proposed FIP protocol, the AODV routing protocol is adopted. When the source node N_s intends to send a message to the destination node N_d that is not its neighboring node, it broadcasts a Route Request (RREQ) message as $\texttt{RREQ} = \langle ID, N_s, N_d, incentInfo, lifeSpan \rangle$, where ID is a sequence number which serves as a unique identifier, N_s, N_d are the source and destination nodes respectively, $incentInfo$ is the incentive information, and $lifeSpan$ is the lifespan of the message.

All nodes receiving this RREQ message will update their information for the source node N_s and set up backwards pointers in the route tables. If the node is not the destination and the RREQ message has not been processed by itself before, it rebroadcasts the RREQ. If a node is either the destination N_d or if it has a route to the destination N_d with the corresponding sequence number greater than or equal to that contained in the RREQ, it responses with a Route Reply (RREP) message to the source node through unicasting, where the intermediate nodes are included.

Fig. 3. A secure ad hoc routing $N_s - N_1 - \cdots - N_n - N_d$ from the source N_s to the destination N_d is assumed having been established based on AODV.

At the end of the AODV routing protocol, a secure route between the source node N_s and the destination node N_d is established. Here, without loss of generality, we assume such a secure ad hoc route is $N_s - N_1 - N_2 - \cdots - N_{n-1} - N_n - N_d$, as shown in Fig. 3. Note that the public key certificate of each involved node can piggyback through the RREQ and/or RREP messages, by which the exchange and verification of public key certificates can be simultaneously accomplished with the route setting.

3) Fair incentive packet forwarding: Once the secure route $N_s - N_1 - N_2 - \cdots - N_{n-1} - N_n - N_d$ is established between N_s and N_d, the source N_s can normally send message m to the destination N_d as follows.

The source node N_s: In order to incent the intermediate nodes $N_1, N_2, \cdots, N_n$ to forward the message m to the destination node N_d, N_s provides an incentive credit message w, which records the following information: "*If the message arrives at the destination N_d, credits values $(n-1)\alpha_c + \beta_c$ will be withdrawn from the source node N_s, deposit credit*

value α_c to each intermediate node N_i, for $i = 1, \cdots, n-1$, and deposit credit value β_c to the last intermediate node N_n." Here, according to the "*work more and get more*" principle, β_c is larger than α_c, for example, $\beta_c = 2\alpha_c$, because the last intermediate node N_n in our mechanism will connect to the TCCS for all intermediate nodes' credit clearance. Note that how to determine the quantity of α_c will be discussed in the later fairness analysis in section IV.

N_s runs the algorithm A1 with the input (m, w), and obtains the returned values (M, σ_1, σ_2), where M is the ciphertext of message m under the static shared key $k_{sd} = x_s Y_d = x_d Y_s = x_s x_d P$, which can provide the confidentiality [21]; σ_1 is the signature of M to achieve the integrity protection; and σ_2 is the verifiably encrypted signature on w, which can provide the non-repudiation on the incentive credit message w. In the end, N_s forwards the packet $(M, w, \sigma_1, \sigma_2)$ to the intermediate node N_1 according to the established route.

Algorithm A1. Source node N_s sends a packet

Input: Plain message m which is launched by source N_s to destination N_d, and the incentive credit message w which is used to pay all the intermediate nodes for the cooperate forwarding.
Output: Encrypted message M and the corresponding authentication messages.

1) compute the static key k_{sd} shared between N_s and N_d as $k_{sd} = x_s Y_d = x_s x_d P$ (pre-computed);
2) encrypt message m as $M = \mathcal{E}(m, k_{sd})$;
3) compute the signature σ_1 on message M and signature σ_2 on message w, where $\sigma_1 = \frac{1}{H(M)+x_s} P$; $\sigma_2 = \frac{1}{H(w)+x_s} Y_T$;
4) return M, σ_1 and σ_2.

Note that the verifiably encrypted signature σ_2 in its current stage is still not a valid standard signature [15], and therefore the intermediate nodes cannot achieve the credit value only based on σ_2. To achieve the credit values, these intermediate nodes must get the receipt from the destination node N_d, so they have to try their best to cooperate forwarding the messages to the destination node.

Algorithm A2. Intermediate node forwarding a packet

Input: Intermediate node N_i, for $i = 1, \cdots, n$, launches the messages M, w, and the authentication messages σ_1, σ_2 and σ_3. (Note: if it is the node N_1, σ_3 is null.)
Output: New authentication message σ_3, which integrates N_i's signature, or $\perp$.

1) compute $e(Y_T, P)$ and $e(P, P)$ (pre-computed), check σ_1 and σ_2 as $e(\sigma_1, H(M)P + Y_s) \stackrel{?}{=} e(P, P)$ and $e(\sigma_2, H(w)P + Y_s) \stackrel{?}{=} e(Y_T, P)$. If *not* both hold, return $\perp$;
2) case **a**: Intermediate node N_1: compute $\sigma_3 = x_1\sigma_1 + x_1 h(N_1)\sigma_2$, return σ_3;
2) case **b**: Intermediate node N_i, for $i = 2, \cdots, n$: check the short aggregated signature σ_3 as follows, $e(\sigma_3, P) \stackrel{?}{=} e(\sigma_1, \sum_{j=1}^{i-1} Y_j) \cdot e(\sigma_2, \sum_{j=1}^{i-1} h(N_j) Y_j)$ If it doesn't hold, return $\perp$; else compute $\sigma_3 = \sigma_3 + x_i\sigma_1 + x_i h(N_i)\sigma_2$ and return σ_3.

The intermediate node $N_1, \cdots, N_n$: When receiving the packet $(M, w, \sigma_1, \sigma_2)$, the intermediate node N_1 invokes the Algorithm A2 to check the validity of σ_1 and σ_2. If they are both valid, N_1 computes the signature $\sigma_3 = x_1\sigma_1 + x_1 h(N_1)\sigma_2$ to prove himself participating the packet forwarding. In the end, N_1 forwards the packet $(M, w, \sigma_1, \sigma_2, \sigma_3)$ to the intermediate node N_2.

On receiving the packet $(M, w, \sigma_1, \sigma_2, \sigma_3)$ from the ancestor N_{i-1}, the intermediate node N_i, for $i = 2, \cdots, n$, also invokes the Algorithm A2 to check the validity of σ_1, σ_2 and σ_3, then recomputes the short aggregated signature σ_3 and forwards the new packet $(M, w, \sigma_1, \sigma_2, \sigma_3)$ to its successor.

Because of the correctness of signatures σ_1, σ_2 and σ_3, the intermediate nodes are willing to forward the packet to the destination node N_d. We should take note that σ_3 is an efficient short aggregated signature [16], which not only has the short signature length, but also with a short signature verification time where the dominant pairing operation is independent of the number of signers to verify. In addition, σ_3 is also provably secure in the standard model. Therefore, it is particularly suitable for the current application scenarios.

The last intermediate node N_n and the destination node N_d: The last interaction between the intermediate node N_n and the destination node N_d is key for our FIP, which is described as follows.

Step 1. Since the destination node N_d is the immediate downstream node of N_n, N_n directly sends the packet $(H(M), w, \sigma_1, \sigma_2, \sigma_3)$ to N_d. Note that for achieving fairness in the protocol, N_d does not send M but its hash value $H(M)$ to N_d in this step.

Step 2. On receiving $(H(M), w, \sigma_1, \sigma_2, \sigma_3)$, N_d first checks the validity of $\sigma_1, \sigma_2, \sigma_3$. If they are all valid, N_d computes the verifiably encrypted signature $\sigma_4 = \frac{1}{H(w)+x_d} Y_T$ and sends it back to N_n.

Step 3. N_n checks the validity of σ_4 by the equation $e(\sigma_4, H(w)P + Y_d) = e(Y_T, P)$. If it holds, the verifiably encrypted signature σ_4 is accepted; otherwise N_n requests a new one from N_d.

Step 4. N_n sends M to the destination node N_d and waits for the receipt of N_d.

Step 5. When receiving M, N_d uses the static shared key k_{sd} to recover m from $M = \mathcal{E}(m, k_{sd})$. Then, N_d computes the signature $\sigma_5 = \frac{1}{H(w)+x_d} P$ as the *receipt*, and sends it back to the intermediate node N_n.

Step 6. N_n checks the validity of σ_5 by $e(\sigma_5, H(w)P + Y_d) = e(P, P)$. If it holds, the signature σ_4 can be accepted. At the end of Step 6, the intermediate node N_n can hold the valid *receipt* (σ_2, σ_5, w), then it can report the *receipt* to the TCCS.

4) Trusted fair credit clearance: As in [11], when the last intermediate node N_n has a fast connection to the TCCS, N_n reports the *receipt* (σ_2, σ_5, w) to the TCCS, then the TCCS applies the Algorithm A3 to perform the fair credit clearance. By converting the verifiably encrypted signature σ_2 to the standard signature σ_6 and checking the validity of the receipt (w, σ_5, σ_6), the TCCS stores the receipt (w, σ_5, σ_6) in the database, withdraws credit values $(n-1)\alpha_c + \beta_c$ from N_s's account, and deposit credit value α_c to each intermediate node N_i for $i = 1, \cdots, n-1$ and β_c to the last intermediate node N_n. The credit balance equation is as follows

$$\begin{cases} N_s \text{ account: } \Psi_s & = \Psi_s - [(n-1)\alpha_c + \beta_c], \\ N_i \text{ account: } \Psi_i & = \Psi_i + \alpha_c, \text{ for } i = 1, \cdots, n-1 \\ N_n \text{ account: } \Psi_n & = \Psi_n + \beta_c. \end{cases}$$

Security. The emergence of bilinear pairing technique makes it possible to develop a secure and efficient short signature scheme. In the proposed FIP, three well-known provably secure short signature schemes are employed [14]–[16], which not only improve the performance but also enhance the overall security of FIP.

Algorithm A3. Trusted fair credit clearance

Input: Input receipt (σ_2, σ_5, w) or message M and receipt $(\sigma_1, \sigma_2, \sigma_4, w)$.
Output: Execute the fair credit clearance, or $\perp$.

1) compute the $e(P, P)$ (pre-computed);
2) case **a**: input is (σ_2, σ_5, w): compute $\sigma_6 = x_T^{-1}\sigma_2$ and check the signature σ_5 and σ_6 as $e(\sigma_5, H(w)P + Y_d) \stackrel{?}{=} e(P, P)$ and $e(\sigma_6, H(w)P + Y_s) \stackrel{?}{=} e(P, P)$. If they do not both hold, return $\perp$. Else check whether the receipt (w, σ_5, σ_6) has existed in the database. If exist, return $\perp$.
2) case **b**: input is $(M, \sigma_1, \sigma_2, \sigma_4, w)$: compute $\sigma_5 = x_T^{-1}\sigma_4$, $\sigma_6 = x_T^{-1}\sigma_2$ and check σ_1, σ_5 and σ_6 as $e(\sigma_1, H(M)P + Y_s) \stackrel{?}{=} e(P, P)$, $e(\sigma_5, H(w)P + Y_d) \stackrel{?}{=} e(P, P)$ and $e(\sigma_6, H(w)P + Y_s) \stackrel{?}{=} e(P, P)$. If they do not both hold, return $\perp$. Else, check whether the receipt (w, σ_5, σ_6) has existed in the database. If exist, return $\perp$. Else send M to the destination node N_d.
3) store the receipt (w, σ_5, σ_6) in the database;
4) withdraw credit values $(n-1)\alpha_c + \beta_c$ from the source node N_s's account, that is, $\Psi_s = \Psi_s - [(n-1)\alpha_c + \beta_c]$;
5) deposit credit value α_c to each intermediate node N_i, for $i = 1, \cdots, n-1$, that is $\Psi_i = \Psi_i + \alpha_c$;
6) deposit credit value β_c to the last intermediate node N_n, that is $\Psi_n = \Psi_n + \beta_c$.

IV. Fairness Analysis

The fairness of FIP is critical for stimulation of selfish nodes. In this paper, the FIP is said to be *fair* if when the protocol runs ends, either the destination node N_d receives the message and the intermediate nodes $N_1, \cdots, N_n$ get credits or neither of them gets anything of interest to them. Based on the atomicity property of fairness and the definitions in Section II-B, we distinguish the outcome of FIP into four states, and analyze the fairness in the following cases.

Case 0 [fair, inexpectant]: STATE 0 $\xrightarrow{no-incent}$ STATE 0.

No stimulation strategy exists in the selfish MANET. Then, the protocol stands STATE 0. In this state, neither the designation node N_d receives M nor the intermediate nodes $N_1, \cdots, N_n$ get the credits. Clearly, this state is *fair*, but the non-cooperative behavior of mobile nodes would result in the sharp degradation of network throughput [7]–[12]. Therefore, the credit stimulation should be introduced to incent the mobile nodes to forward the packets.

To ensure the packet forwarding work well, it is important to incent each selfish intermediate node to work. Thus, we quantitatively analyze the success probability of the packet forwarding under the credit stimulation strategy. According to the common sense, we define that the intermediate node's *selfish ratio* (SR) is inverse to the quantity of incentive credits x. That is, $SR = \frac{1}{c_o \cdot x}$, where $c_o (> 1)$ is a constant coefficient.

Assume there are totally n intermediate nodes N_1, N_2, $\cdots$, N_n along the pre-defined route. Based on the stimulation strategy, for each intermediate node N_i, where $i = 1, \cdots, n-1$, the SR is $\frac{1}{c_o \cdot \alpha_c}$, and the probability that this intermediate node is willing to forward the packet is $1 - \frac{1}{c_o \cdot \alpha_c}$. With the same reason, the probability that the last intermediate node N_n would like to forward the packet is $1 - \frac{1}{c_o \cdot \beta_c}$. So the probability that packet forwarding work well is

$$Pr = \left(1 - \frac{1}{c_o \cdot \alpha_c}\right)^{n-1} \cdot \left(1 - \frac{1}{c_o \cdot \beta_c}\right) \quad (1)$$

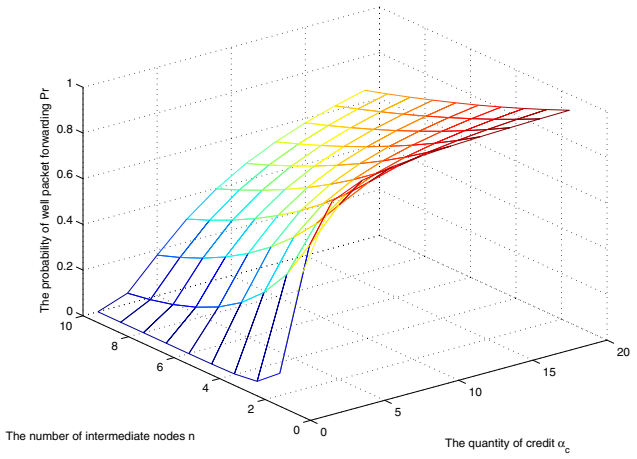

Fig. 4. The probability of well packet forwarding in FIP protocol under different n and different α_c, where $1 \le n \le 10$, $1 \le \alpha_c \le 20$

When we assume $c_o = 1.2$ and $\beta_c = 2\alpha_c$, Fig. 4 illustrates the probability Pr varies with n (the number of intermediate nodes) and α_c (the quantity of credit), where $1 \le n \le 10$ and $1 \le \alpha_c \le 20$. It can be observed that the packet forwarding can work well with the increase of the quantity of α_c and in inverse proportion to the number of the intermediate nodes n. In addition, to achieve a good packet forwarding probability, when knowing the number of intermediate nodes and assuming $\beta_c = 2\alpha_c$, the source node N_s can compute the credit value of α_c by solving the Eq. (1), and determine withdrawing credits $(n-1)\alpha_c + \beta_c$ from its account.

Case 1 [fair, expectant]: STATE 0 $\xrightarrow{incent}$ STATE 1.

A credit stimulation strategy exists in the selfish MANET. Both the intermediate nodes $N_1, \cdots, N_n$ and the source / destination nodes N_s, N_d are honest and properly carry out the FIP. Then, the FIP will terminate after N_n receives and checks the standard signature σ_5, and the outcome stands STATE 1. It is straightforward to prove that this state is expectant and fair, since N_d receiving M and N_n will obtain the standard signature σ_5. Withholding the valid receipt (σ_2, σ_5, w), the intermediate nodes can get the credit by connecting with the TCCS. Then, the TCCS invokes the Algorithm A3 to execute the trusted credit clearance.

Case 2 [unfair, inexpectant]: STATE 0 $\xrightarrow{incent}$ STATE 2.

A credit strategy exists in the selfish MANET. The intermediate nodes $N_1, \cdots, N_n$ are honest, however, the source / destination may become selfish and collude to deny paying

the credit after the packet reaches the destination. With the FIP, this case takes place at the protocol termination before N_d sends σ_5 to N_n, the outcome of FIP stands STATE 2. In this state, N_d gets M but N_n does not receive the standard signature σ_5. Clearly, this state is *unfair* to the intermediate nodes. Therefore, the fairness is required. In our FIP, since the intermediate node N_n cannot receive a valid receipt σ_5, it reports $(M, \sigma_1, \sigma_2, \sigma_4, w)$ to the TCCS when it has a fast connection to the latter. As described in Algorithm A3, the TCCS first converts the verifiably encrypted signatures σ_4, σ_2 into the standard signatures σ_5, σ_6, and checks the validity of $\sigma_1, \sigma_5, \sigma_6$. If all these signatures are valid, the TCCS would still like to withdraw credit values from the source node N_s and deposit credit values to each intermediate node N_i for $i = 1, \cdots, n$ according to the incentive credit message w. Therefore, the *fairness* is achieved. Note that the TCCS still sends M to the destination node N_d in this case, since the FIP should be able to tackle the selfish intermediate nodes, which will be discussed in the next case.

Case 3 [fair, inexpectant]: STATE 0 $\xrightarrow{incent}$ STATE 3.

A credit stimulation measure exists in the selfish MANET. The source / destination nodes N_s, N_d behave normally, but the intermediate nodes are still selfish potentially. In this case, our FIP terminates before the last intermediate node N_n sends M to the destination node N_d, and the outcome of FIP stands STATE 3, which means that the intermediate node N_n receives σ_4 but the destination node N_d does not receive M. Therefore, it seems unfair to N_d. However, since σ_4 is not a standard signature but a verifiably encrypted signature, the intermediate nodes cannot get the credits, and thus this state is still *fair*. In order to get the credits, the last intermediate node has to connect to the TCCS with the report $(M, \sigma_1, \sigma_2, \sigma_4, w)$. Then, as in case 2, the intermediate nodes can get their credits. However, the TCCS also sends M to the destination node N_d simultaneously, and thus the selfish behavior of the intermediate node N_n brings it no advantage. Besides, the selfish behavior of N_n also wastes its limited storage to store M. Therefore, the last intermediate node N_n will try its best to forward the packet M. As a result, due to the incentive strategy of FIP, this selfish case is preventive.

Note. The occurrence of case 2 or case 3 may not be due to the selfish behaviors of mobile nodes, but could be because of the unreliable channels between the last intermediate node N_n and the destination node N_d. From such a viewpoint, the FIP also improves reliability of the last hop, where the packet M in an unreliable channel could be delayed but will eventually arrive to the destination node N_d.

V. Conclusion and Future Work

In this paper, we presented a novel fair incentive protocol FIP to provide incentive to mobile nodes to cooperate in selfish MANETs. The proposed FIP is carefully designed, which does not require any tamper-resistant device but achieve the fairness between the source /destination nodes and intermediate nodes. Through a careful analysis in fair incentive state transition model, FIP has demonstrated the required fairness characteristics. As our future research efforts, we will conduct extensive simulation to evaluate the performance and integrate FIP with anonymity to provide mobile nodes' privacy protection [22].

References

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

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

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. of The Sixth International Conference on Mobile Computing and Networking Networking (MobiCom 2000)*, Boston, MA, Aug. 2000. pp. 255-265.

[4] S. Buchegger and J.-Y. L. Boudec, "Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks," in *Proc. 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing, 2002*, Canary Islands, Spain, Jan. 2002, pp. 403-410.

[5] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol: Cooperation of nodes - fairness in dynamic ad-hoc networks," in *Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc 2002)*, Lausanne, Switzerland, Jun. 2002, pp. 226-236.

[6] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," in *Proc. of IEEE WCNC 2003*, Vol. 3 New Orleans, LA, March 2003, pp. 1510-1515.

[7] L. Buttyan and J. P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *Proc. of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHoc 2000)*, Boston, MA, Aug. 2000, pp. 87-96.

[8] L. Buttyan and J.-P. Hubaux, "Stimulating cooperation in self- organizing mobile ad hoc networks," *ACM/Kluwer Mobile Networks and Applications*, Vol. 8, No. 5, pp. 579-592, 2003.

[9] J.-P. Hubaux, T. Gross, J.-Y. L. Boudec, and M. Vetterli, "Toward self-organized mobile ad hoc networks: the terminodes project," *IEEE Communications Magazine*, Vol. 31, No. 1, pp. 118-124, Jan. 2001.

[10] M. Jakobsson, J.-P. Hubaux, and L. Buttyan, "A micropayment scheme encouraging collaboration in multi-hop cellular networks," in *Proc. FC 2003*, LNCS 2742, pp. 15-33, Springer-Verlag, 2003.

[11] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. INFOCOM 2003*, Vol. 3, Mar.-Apr. 2003, pp. 1987-1997.

[12] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks", *Wireless Networks (WINET)*, Vol 13, No. 5, October 2007.

[13] N. Asokan, M. Schunter, and M. Waidner, "Optimistic protocols for fair exchange", in *Proc. of the 4st ACM conference on Computer and Communications Security (CCS) 1997*, Zurich, Switzerland, April 1997, pp. 7-17.

[14] F. Zhang, R. Safavi-Nani, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications", in *Proc. PKC 2004*, LNCS 2947, pp. 277-290, Springer-Verlag, 2004.

[15] F. Zhang, R. Safavi-Nani, and W. Susilo, "Efficient verifiably encrypted signature and partially blind signature from bilinear pairings", in *Proc. INDOCRYPT 2003*, LNCS 2904, pp. 191-204, Springer-Verlag, 2003.

[16] J. Camenisch, S. Hohenberger, and M. Pedersen, "Batch verification of short signatures", in *Advances in Cryptology - EUROCRYPT 2007*, LNCS 4515, pp. 246-263, Springer-Verlag, 2007.

[17] H. Pagnia and F.C. Gartner, "On the impossibility of fair exchange without a trusted third party", *Tech. Rep. TUD-BS-1999-02*, Darmstadt University of Technology, March, 1999.

[18] *International Standard ISO/IEC 8802-11*, ANSI/IEEE Std 802.11, 1999 Edn.

[19] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", in *Advances in Cryptology - CRYPTO 2001*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[20] C. E. Perkins, E. M. Royer, "Ad-hoc on-demand distance vector routing", in Proc. Second IEEE Workshop on Mobile Computer Systems and Applications, 1999, pp. 90-100.

[21] W. Diffie and M. Hellman, "New directions in cryptography", *IEEE Transaction on Information Theory*, Vol. 22, pp. 644-654, 1976.

[22] X. Lin, X. Sun, P. H. Ho, and X. Shen, "GSIS: a secure and privacy preserving protocol for vehicular communications", *IEEE Transaction on Vehicular Technology*, Vol. 56, No. 6, pp. 3442-3456, 2007.