SATs: Secure Data-Forwarding Scheme for Delay-Tolerant Wireless Networks
Mohamed Elsalih Mahmoud, Mrinmoy Barua, and Xuemin (Sherman) Shen
Department of Electrical and Computer Engineering
University of Waterloo, Waterloo, Ontario, Canada, N2L 3G1

Abstract—In this paper, we propose a secure data-forwarding scheme, called SATs, for delay-tolerant wireless networks. SATs uses credits (or micropayment) to stimulate the nodes’ cooperation in relaying other nodes’ messages and to enforce fairness. SATs also makes use of a trust system to assign a trust value for each node. A node’s trust value is high when the node actively forwards others’ messages. The highly trusted nodes are preferable in data forwarding to avoid the Black-Hole attackers that drop messages intentionally to degrade the message delivery rate. In this way, SATs can stimulate the nodes’ cooperation not only to earn credits but also to maintain high trust values to increase their chances to participate in future data forwarding. Our security evaluation demonstrates that SATs can secure the payment and trust calculation. The performance evaluation demonstrates that SATs can significantly improve the message delivery rate due to avoiding the Black-Hole attackers in message forwarding and stimulating the nodes’ cooperation.

Index Terms—Black-Hole attacks, cooperation incentive scheme; secure data-forwarding schemes; security; trust systems.

I. INTRODUCTION

Delay-tolerant wireless networks (DTNs) [1] are a new class of networks characterized by long message delivery delay and lack of fully connected path between the source and destination nodes. As a result, message forwarding follows a store-carry-and-forward approach where the mobile nodes, acting as message carriers, buffer in-transit messages until the next node in the path appears, e.g., a new node moves into the range, and so on, until the messages reach their destinations. This message-forwarding scheme is an opportunistic one because messages are forwarded in an opportunistic way.

Wide range of useful applications have been developed for DTNs. Pocket-switched DTNs take advantage of the increasing popularity of the mobile devices equipped with wireless network interface to enable a new class of social networking applications [2]. DTNs can be readily deployed at low cost to provide Internet service to remote and developing areas. Vehicular DTNs can be used for dissemination of location-dependent information such as local ads, traffic reports, and parking information [3]. However, the practical implementation of DTNs is questionable because the networks’ unique characteristics have made them vulnerable to serious security threats.

The existing message-forwarding schemes assume that the intermediate nodes (or carriers) will follow the schemes faithfully. However, if carriers misbehave, the network performance and connectivity severely degrade, which may fail the multi-hop communication. The DTNs rely on the essential requirement that the carriers cooperate in forwarding others’ messages. This requirement cannot be guaranteed because the selfish nodes will not spend their precious resources to forward others’ messages without compensation, and the malicious nodes may launch Black-Hole attack by dropping the messages intentionally. Moreover, the fairness issue arises when the selfish nodes take advantage of the honest nodes without contributing to them. Thwarting the Selfishness and Black-Hole attacks is a real challenge due to the un-connectivity and distributed nature of the DTNs.

In this paper, we propose a Secure dATa-forwarding Scheme for delay-tolerant wireless networks called SATs to thwart the Selfishness and Black-Hole attacks. To thwart the Selfishness attacks, the source node pays credits (or micropayments) to the intermediate nodes for relaying their packets. Credits not only stimulate the nodes’ cooperation but also enforce fairness because they can compensate the nodes for the consumed resources in message forwarding. Moreover, most of the existing message-forwarding schemes make forwarding decisions solely based on the probability that a carrier can deliver the message to the destination node. It is important also to select a trusted node as a message carrier to increase the message delivery rate as well as to reduce the message delivery delay. Different from these schemes, SATs considers both the probability of delivering the messages and the carriers’ trust values. SATs makes use of a trust system to assign a trust value for each node. A node’s trust value is high when it actively forwards others’ messages. The highly trusted nodes are preferable in message forwarding to avoid the Black-Hole attackers that intentionally drop messages. In this way, SATs stimulates the nodes’ cooperation not only to earn credits but also to maintain high trust values to increase their chances to participate in future message forwarding. In other words, if a node does not cooperate for some time or frequently drops messages, its trust value degrades and thus its chance to be involved in future message-forwarding decreases.

Our security evaluation demonstrates that SATs can secure the payment and trust calculation. The performance evaluation demonstrates that SATs can significantly improve the message delivery rate due to avoiding the Black-Hole attackers in message forwarding and stimulating the nodes’ cooperation. The main contributions of this paper can be summarized as follows: (1) To the best of our knowledge, SATs is the first scheme that can thwart both Selfishness and Black-Hole attacks in DTNs; (2) we propose a novel trust system to maintain a trust value for each node in the network; and (3) We program a simulator to estimate the message delivery rate with and without our scheme.

The remainder of this paper is organized as follows. We review the related work in Section II. In Section III, we present the network and threat models. We propose SATs in Section IV. Security analysis and performance evaluation are given in Sections V and VI, respectively, followed by conclusion and future work in Section VII.
II. RELATED WORK

A. Ad Hoc Wireless Networks

In [4], the source node signs the identities of the nodes in the route and attaches the signature to each message and the destination node replies with a signed ACK. The intermediate nodes compose undeniable proof of message forwarding, called payment receipt, which contains the identities of the payers and the payees, and the payment amount. The nodes submit the receipts to a centralized unit, called the trusted party (Tp), to update their accounts. In [5], each node submits brief payment reports containing the alleged charges and rewards for different sessions. The payment of the fair reports can be cleared with almost no processing overhead. Statistical methods are used to identify the cheating nodes that report incorrect payment. Unlike the proposed schemes in [4, 5] which stimulate the nodes’ cooperation, the proposed scheme in [6] aims to enforce cooperation. 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 A overhears the medium to make sure that B relays the packet. A increases the reputation value of B when it overhears the packet transmission; otherwise, A decreases the reputation value of B. Node A accuses B of un-cooperation as soon as its reputation value degrades beyond a threshold. Based on the watchdog’s accusations, the path-rater module chooses the path that avoids the uncooperative nodes.

However, the proposed schemes for the mobile ad hoc networks are not applicable for DTNs for the following reasons. First, the incentive schemes such as [4, 5] usually require establishing a full end-to-end route between the source and the destination nodes before the data transmission occurs. This assumption does not hold for DTN because messages are opportunistically forwarded. Second, message transmission cannot be monitored in DTNs because the nodes forward the messages shortly after receiving them in the ad hoc networks but DTNs use store-carry-and-forward approach, i.e., a node has to wait until the next node in the path appears.

B. Delay Tolerant Wireless Networks

In [7], the simulation results show that the selfish nodes can greatly degrade the message delivery rate in DTNs. To mitigate the damage caused by selfish nodes, the pair-wise tit-for-tat (TFT) has been used as a simple, robust, and practical incentive scheme for DTNs. The scheme allows selfish nodes to maximize their individual utilities while conforming to TFT constraints. Simulation results are given to show that the scheme can increase the total delivered traffic in the network.

In [8], Zhu et al. propose a multilayer incentive scheme, called SMART, for DTNs. Layered coins are used to provide incentives to selfish nodes for message forwarding. Compared to the proposed scheme in [7], SMART pays more attention to securing the payment, i.e., SMART is robust against new attacks such as Credit-Forgery, Nodular-Tontine, and Submission-Refusal attacks. Different from SMART, Lu et al. [9] propose an incentive scheme for DTNs, which focuses on the fairness issue. To achieve fairness, the intermediate nodes are rewarded if the messages reach to the destination node, and for the failure of message delivery, the intermediate nodes that forwarded the undelivered messages are preferable in the future message forwarding. However, unlike SATS that aims to thwart the Selfishness and Black-Hole attacks, the existing schemes only stimulate the selfish nodes’ cooperation.

In [10], the concept of encounter tickets is introduced to ensure that the nodes provide correct information regarding the probabilities of contacting other nodes. However, the proposed scheme can only prevent the attackers from claiming non-existent encounters and cannot thwart Black-Hole attack. The proposed schemes in [11, 12] rely on the introduction of a trusted examiner, called ferry node, to thwart Black-Hole attack. The ferry node moves around in the network and validates the message delivery probability to determine the presence of the Black-Hole attack, but these schemes cannot stimulate the nodes’ cooperation.
nodes are stimulated (not forced) to forward others’ messages, and thus the nodes can self-determine whether to participate in message forwarding.

Our payment model adopts paying per message, which means that if $n$ carriers forward a message until it reaches to the destination, each of $n$ carriers should receive $\lambda$ credits, whereas the source node pays $\lambda \times n$ in total. The source node is charged and the carriers are rewarded if and only if the destination node receives the messages. The source node can restrict the amount of credits it may pay for a message by deciding the maximum number of hops (N) to deliver a message to the destination. The nodes having low delivery probabilities, such as those at the network border and the low-mobile nodes, cannot earn as many credits as the other nodes because they are less frequently selected by the message-forwarding scheme. To enable these nodes to communicate, they can purchase credits for real money from $T_p$.

**B. Threat and Trust Models**

The attackers have full control on their nodes and thus they can change the nodes’ operations. In this work, we focus on the attacks launched by individual attackers. Collusion attacks will be studied in our future work. Specifically, the attackers aim to steal credits, pay less, communicate freely, and falsely improve their trust values. $T_p$ is fully secure because it is run by a single operator that is motivated to ensure the network security, but the mobile nodes are probable attackers because they are autonomous and self-interested.

In DTNs, the nodes do not have a priori knowledge of the network connectivity, so in most of the existing data-forwarding schemes, each node has to estimate the probability of contacting other nodes in the future based on the past experiences, which is called delivery probability. However, the mobile nodes provide these probabilities and it is difficult to verify them due to the network un-connectivity. The malicious nodes may disseminate false delivery probabilities in undetectable way to surreptitiously increase, or decrease, their chances to be selected as next-hop nodes. For example, a node may disseminate large delivery probability to increase its chance to be chosen and thus increases its ability to attract messages to gain more credits (but on the expense of increasing the delivery delay), or to launch **Black-Hole** attacks by dropping the messages as shown in Fig. 2. The **Black-Hole** attackers aim to cause a severe drop in the message delivery rate or to launch **Eavesdropping** or **Selective-Forwarding** attacks. On other hand, if an incentive protocol is not used, the selfish nodes may disseminate low delivery probabilities so that the other nodes never choose them in message forwarding to save their resources. For the trust models, the nodes trust $T_p$ with performing billing and trust calculation, but they do not trust the mobile nodes.

![Fig. 2: The Black-Hole attack.](image)

**IV. THE PROPOSED SATS**

SATS consists of three phases: **Message Generation**, **Message Delivery**, and **Trust and Credit Update**.

**A. Message Generation**

For each message $M$, the source node (S) sends the data packet shown in Fig. 3. $T_s$ is the message generation timestamp and $N$ is the maximum hop count that limits the number of intermediate nodes and thus limits the amount of payment for delivering the message to $\lambda \times N$. The message should be delivered within a particular time-to-live (TTL) period. $H(M)$ and $L$ are the message’s hash value and length, respectively. The source node’s signature $(\text{Sig}_s())$ is important to ensure the packet’s integrity and authenticity to secure the payment. $T_m$ is the minimum trust value a node can have to act as carrier for the message. The source node’s certificate $(C_s)$ is attached to enable the nodes to verify its signature. The source node sends the packet to the neighbor that has the maximum probability to deliver the message to the destination node (D) and its trust value is at least $T_m$.

**B. Message Delivery**

The nodes in DTNs usually exhibit repetitive motions in nature. Several recently proposed schemes have utilized this repetitive nature for predicting future message forwarding based on the gathered history information. Messages are opportunistically forwarded towards the destinations using prediction metrics computed from the nodes’ contact history. The underlying idea is that if two nodes have come in contact many times before, the likelihood of their encounter in the future is considered to be high. SATS can be incorporated with any data-forwarding protocol but in selecting the next hop node, SATS considers the nodes’ trust values alongside with the probabilities that the nodes can deliver the message. In this paper, we implement SATS on the top of PROPHET data-forwarding protocol [13]. PROPHET uses Eqs. 1, 2, and 3 to update the delivery probabilities. The node $A$ updates its probability to contact node $B$ ($P_{AB}(t)$) whenever it contacts $B$ using Eq. 1, where $\alpha$ is an initialization constant and $\alpha \in [0, 1]$. If the nodes $A$ and $B$ do not contact each other for a time interval, node $A$ would update its delivery probability to $B$ using Eq. 2, where $\gamma$ is the aging constant and $\gamma \in [0, 1]$. Moreover, the delivery probability also has a transitive property. When node $A$ contacts $B$ which encountered node $C$ previously, node $A$ updates its delivery probability to node $C$ based on the delivery probabilities of $P_{AC}(t)$ and $P_{BC}(t)$ using Eq. 3, where $\beta$ is a scaling constant that controls the impact of the transitivity value on the delivery predictability.

\[
P_{AB}(t) = P_{AB}(t-1) + \alpha \times (1 - P_{AB}(t-1)) \tag{1}
\]

\[
P_{AB}(t) = P_{AB}(t-1) \times \gamma^k \tag{2}
\]
\[ P_{AC}(t) = P_{AC}(t-1) + (1 - P_{AC}(t-1)) \times P_{AB}(t) \times P_{BC}(t) \times \beta \] (3)

When an intermediate node receives the packet, it performs the following steps: (1) Checks if the packet is in its lifetime, i.e., current time < TTL + Ts; (2) Checks if the number of intermediate nodes is fewer than N; and (3) Verifies the signature chain to ensure that the message has been indeed forwarded by the nodes listed in the packet. After performing the aforementioned verifications, the node buffers the message and carries it until it meets the destination node or another node with higher probability of contacting the destination node. For example, Fig. 4 shows that when node A meets another node B that has higher probability of meeting D and its trust value is at least \( T_{m} \), A replicates and forwards the packet to B. The intermediate node A signs the signature chain and forwards the packet after adding its identity and certificate as shown in Fig. 3. Figs. 3 and 4 show that node B acts as A and delivers the message to the destination. Therefore, the message forwarding follows a “store-carry-and-forward” manner and it is opportunistically forwarded from one intermediate node to another until it reaches the destination through intermittent connections. Upon receiving the message, the destination node signs the signature chain (\( A_D \)) to generate \( A_{D'} \), where \( A_D = \text{Sig}_D(A_N) \), and transmits \( A_{D'} \) to node B.

\[ \text{Pr}(t \leq n) = 1 - (\prod_{i=0}^{N-1} \psi_{i-1}^{-C-1})^n \] (4)

We define a node’s trust value as a real number in the range of \([0, 1]\), with 1 indicating complete trust and 0 complete distrust. The nodes’ signatures enable Tp to ensure that the listed nodes in a receipt have been indeed participated in forwarding the message. This is important to secure the payment and trust calculation. \( T_i(t) \) refers to the trust value of node i at time t. \( T_i(t) \) is low for the Black-Hole attackers and the less cooperative nodes but it is high for the normal nodes that actively forward others’ messages. The underlying idea of the trust system is that if the destination node receives a message, then the carriers that have forwarded the message are not misbehaving or, otherwise, the destination node would have not received the message. Therefore, for each delivered message, Tp increases the trust values of the carriers that forwarded the message. SATS aims to identify the good nodes and forward the messages through them, and thus SATS can avoid the Black-Hole attackers in message forwarding and punish them by not earning credits.

Eq. 5 can calculate a node’s trust value. \( T_i(t-1) \) is the trust value of node i at time t-1 or the old trust value, \( \mu \) is the rate at which the trust value would decrease, \( T_i(\tau) \) is the node’s trust value in the time interval \( \tau \), where \( T_i(\tau) = \frac{N}{M} \cdot N \) is the number of delivered messages that node i forwarded in \( \tau \) and \( M \) is a normalizing factor that depicts the maximum number of delivered messages that a trusted node can forward in \( \tau \). Note that the maximum value of \( T_i(\tau) \) is 1 and thus \( T_i(\tau) = 1 \) if \( \frac{N}{M} > 1 \). From Eq. 5, a node’s trust value decreases over time if the node does not forward others’ messages, e.g., if \( T_i(\tau) = 0, T_i(t) = e^{-\mu \tau} \times T_i(t-1) < T_i(t-1) \). The larger
\( \mu \) is the quicker \( T_i(t) \) decreases. Therefore, in order to keep good trust value, the nodes should not stop forwarding others’ messages. The centralized trust system can compute a good value for \( M \) by observing the maximum number of messages the nodes forward in \( \tau \) time window.

\[
T_i(t) = e^{-\mu \tau} \times T_i(t - 1) + \left(1 - e^{-\mu \tau}\right) \times T_i(\tau)
\]  

(5)

V. SECURITY EVALUATION

In Double-Rewarding attack, the attacker attempts to clear a receipt multiple times to increase its rewards. \( Tp \) can thwart the attack because it verifies whether a receipt has been cleared before. For Double-Spending attack, the attacker attempts to generate identical receipts for different sessions to pay once. For Ferguson-and-Manipulation attack, the attacker attempts to forge receipts or manipulate valid receipts to increase their rewards. This is not possible in SATS with using secure public-key cryptography because it is not possible to forge or modify the nodes’ signatures and compute the private keys from the public ones. For Free-Riding attacks, two colluding intermediate nodes may manipulate packets to piggybacking their data to communicate freely. This attack is not possible in SATS because the source node’s signature can protect the message’s integrity and the packet integrity is checked at each node and thus the first node after the packet manipulation can detect the manipulation and drop the packet. It is obvious that launching this attack is only possible when there is at least one honest node residing between the two colluders because the colluding nodes can directly exchange messages without the aid of others if they are neighbors.

In Packet-Replay attack, the attackers record valid packets and replay them in different place and/or time claiming that they are fresh to transmit their messages under the names of others. This attack is not possible because the attackers cannot forge the source node’s signature for a fresh timestamp. For Message-and-Payment-Repudiation attacks, the attacker attempts to deny transmitting a message or the payment so as not to pay. The non-repudiation property of the source node’s signature can protect the message’s integrity and the packet integrity is checked at each node and thus the first node after the packet manipulation can detect the manipulation and drop the packet. It is obvious that launching this attack is only possible when there is at least one honest node residing between the two colluders because the colluding nodes can directly exchange messages without the aid of others if they are neighbors.

The cheating node that submits incorrect descriptors can be identified and evicted once \( Tp \) detects one cheating action. Moreover, the node cannot know which evidences will be requested by \( Tp \) because evidences are randomly selected, and the number of cheated descriptors can be probabilistically restricted. In Layer-Adding attack, the attackers aim to add layers to the signature chain to reward other nodes without participating in message forwarding. This is not possible if each node has a unique identity and public/private keys. In our scheme, if a node lies in its message delivery probability, e.g., to attract more messages and then drop some of these messages instead of forwarding them, the messages will not reach to the destination and the nodes lose both trust and credit. Receiption-Submission-Refusal attack, the last intermediate node may collude with the source node so as not to submit the receipt and receive behind-the-scene compensation from the source. Due to the lack of end-to-end connection, the source node and other intermediate nodes cannot know the last intermediate node. The nodes can communicate even if they do not have sufficient credits at the communication time, so to limit overspending, certificate lifetime is short and depends on the node’s available credits and its average credit consumption rate.

The objectives of implementing trust in message forwarding are as follows: (1) To foster trust among the nodes by making knowledge about the nodes’ past behaviors available; (2) To encourage the nodes to participate actively in forwarding others’ messages; (3) To encourage the nodes to tell the truth about their message delivery probabilities; and (4) To punish the nodes that frequently drop the messages because any loss of trust means loss of potential earnings. SATS can precisely compute the nodes’ trust values because the centralized trust system can observe the nodes’ behaviors over long time. Trust systems are susceptible to collusion attacks due to the nature of these systems. For example, the colluding nodes may launch Trust-Boost attacks by composing receipts for fake message transmission to improve their trust values. This attack can be discouraged by imposing fees to clear the payment, i.e., the nodes lose credits when launching this attack. For Trust-Degradation attack, the attackers drop the messages when they observe that the victim nodes have participated in the message forwarding to degrade the victim nodes’ trust values. First, this attack does not always work because the attackers may not participate in message forwarding. Second, the attackers lose both trust and credits, which may discourage the attack. Finally, frequently launching this attack reduces its effectiveness because the attackers’ trust values degrade and thus they are less frequently selected in message forwarding.

VI. PERFORMANCE EVALUATION

In this section, we evaluate the proposed scheme using a simulator built with Matlab. The performance metric used in the evaluation is the message delivery rate, which is the ratio of generated messages that are correctly delivered to the destination nodes within a given time interval. In our simulation, we randomly deploy 70 nodes in a square area of 1200 m × 1200 m. The transmission range of each node is 150 m. During each experimental run, we randomly select 10 pairs of nodes to communicate with each other. The packet size is 10 KB and the buffer size at each node is 70 packets. To simulate the nodes’ mobility, we have considered a human mobility model based on social network theory [14]. The model is able to generate movements that are based on the strength of the relationships between the people carrying the devices. Each data point is the average of 20 runs. The Black-Hole attackers drop all the packets they receive.

We simulate PROPHET protocol with and without our mitigation scheme. In our simulations, a Black-Hole attacker is always an intermediate node, while an honest node can be a source, a destination, or an intermediate node. Since each message has a lifetime, the messages that are not delivered within the lifetime are dropped. Moreover, the nodes do not accept new packets when the buffer is full. The message
generation rate is 12 messages/hr. Table I summarizes the simulation parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of nodes</td>
<td>70 nodes</td>
</tr>
<tr>
<td>Network size</td>
<td>1200 m × 1200 m</td>
</tr>
<tr>
<td>Speed of nodes</td>
<td>1.5 m/s</td>
</tr>
<tr>
<td>Transmission range</td>
<td>150</td>
</tr>
<tr>
<td>Mobility model</td>
<td>Based on social network theory [14].</td>
</tr>
<tr>
<td>Packet size</td>
<td>10 KB</td>
</tr>
<tr>
<td>Message generation interval</td>
<td>12 messages/hr</td>
</tr>
<tr>
<td>The maximum hop count (N)</td>
<td>5</td>
</tr>
<tr>
<td>α, β, and γ</td>
<td>0.75, 0.25, and 0.98</td>
</tr>
<tr>
<td>Buffer size</td>
<td>70</td>
</tr>
</tbody>
</table>

The maximum hop count (N) 5
Message generation interval 12 messages/hr
Packet size 10 KB
Mobility model Based on social network theory [14].
Transmission range 150
Speed of nodes [1, 5] m/s
Network size 1200 m × 1200 m
Number of nodes 70 nodes

Black-Hole
Black-Hole
Black-Hole
Black-Hole
Black-Hole

Fig. 6: The delivery rate VS. time (in minutes) at 20 Black-Hole attackers.

Fig. 7: The delivery rate VS. the number of Black-Hole attackers at t = 800 minutes.

Fig. 6 shows the average message-delivery rate versus time (in minutes) for PROPHET protocol with and without SATS and with 20 Black-Hole attackers. From the figure, we can see that SATS is able to improve the message delivery rate due to avoiding the Black-Hole attackers in message forwarding. As time passes, more messages are delivered with and without SATS but the message-delivery rate is higher in SATS.

Fig. 7 shows the message delivery rate versus the number of Black-Hole attackers at t = 800 minutes. The figure shows that the increase of the Black-Hole attackers significantly decreases the message delivery rate without SATS because the protocol cannot make smart decisions regarding node selection, i.e., it involves the Black-Hole attackers in message forwarding. However, with SATS, the message delivery rate is higher because SATS is able to avoid the Black-Hole attackers and select good nodes to forward the messages. With a large ratio of the Black-Hole attackers, the message delivery ratio severely degrades without using SATS because our scheme is able to avoid the Black-Hole attackers in message forwarding.

VII. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a novel data-forwarding scheme for delay-tolerant wireless networks, which combines the message-delivery probability and the notion of trust. Credits are used to stimulate the nodes’ cooperation and enforce fairness, and trust values are integrated to the message-forwarding decisions to avoid the Black-Hole attackers. Our simulations confirm that SATS can improve the message delivery rate due to stimulating the selfish nodes’ cooperation and avoiding the Black-Hole attackers in message forwarding. The security evaluations have shown that SATS can secure the payment and trust calculation. For our future work, we will integrate SATS with anonymity to provide privacy protection to the DTN nodes. We will also study collusion attacks launched by malicious nodes.

REFERENCES


