PROPOSED SECURITY MODEL

The current chapter discusses about the proposed model for the purpose of mitigating the malicious behaviour of the mobile nodes in Mobile Adhoc Network. The chapter mainly introduces and elaborates the proposed models and design goal along with description of node Model and proposed protocol with support of algorithm execution.

4.1 INTRODUCTION

The opportunistic data propagation in opportunistic networks has been well studied so far, and several efficient opportunistic routing protocols have been proposed under the hypothesis that each individual opportunistic network node is willing to forward bundles for others (Spyropoulos, 2008). However, when opportunistic network nodes are controlled by rational entities, such as human or organization (Burgess, 2000) (Chaintreau, 2006), some opportunistic network nodes will behave selfishly and may not be willing to help others to forward bundles, so the hypothesis will be violated (Upendra, 2008) (Zhu, 2009). For example, in order to conserve power, buffer and computing resources, a selfish opportunistic network node may be reluctant in the cooperation that is not directly beneficial to it, which could make a well designed opportunistic routing useless. Therefore, how to efficiently and effectively resolve the selfishness problem in opportunistic networks has become a very challenging issue to achieve better packet delivery performance of opportunistic networks. To stimulate
forward packets, many reputation-based and credit-based enticement protocols for wireless ad hoc network have been proposed (Marti, 2000) (Buchegger, 2002) (Liu, 2003) (Buttyan, 2000) (Hubaux, 2001) (Zhong, 2003) (Zhang, 2007) (Mahmoud, 2010). However, due to the unique features of opportunistic networks, such as the lack of contemporaneous path and high variation in network conditions, it is hard to detect opportunistic network nodes’ selfish behaviors or predetermine a routing path. Therefore, these challenges in opportunistic networks make the existing security protocols, which usually rely on a contemporaneous routing, not applicable to opportunistic networks. In this study, in order to improve the performance of the opportunistic networks in terms of high delivery ratio and low average delay, we propose a security based packet forwarding protocol to address the selfishness problem in opportunistic networks. In the proposed protocol, when the source opportunistic network node sends a bundle, it doesn’t set a routing path in advance, but only need to attach some enticement on the bundle. Then, the selfish opportunistic network nodes on the road could be stimulated to help with forwarding the bundle to improve the delivery ratio and reduce the average delay of the whole opportunistic networks. Specifically, the contributions of this proposed study are threefold. A

- First, we provide a fair enticement model in which selfish opportunistic network nodes are stimulated to help forward bundles with credit-based enticement as well as reputation-based enticement.
In the reward model, to achieve fairness, if and only if the bundles arrive at the destination node, the intermediate forwarding nodes can get credits from the source node.

- Furthermore, for the failure of bundle forwarding, those intermediate forwarding nodes still can get good reputation values from a trusted authority (TA). Therefore, with this stimulation, the packet delivery performance of opportunistic networks can be improved.

- Second, in order to guarantee the feasibility of the fair enticement model, we use the verifiably encrypted signature techniques in order to provide authentication and integrity protection in the proposed security based packet forwarding protocol.

- Third, to confirm the effectiveness of the proposed security based packet forwarding protocol, we also develop a custom simulator built in Java to substantially show that the proposed security based packet forwarding protocol can achieve the high delivery ratio and low average delay of opportunistic networks when the high enticement is provided.

### 4.2 PROPOSED MODEL

This prime aim of the work is to establish the fundamentals to implement in the future security so that mobile adhoc protocol can also thwart various attacks, which could be launched by certain malicious nodes that originate due to routing issue in MANET. The current work is addressed keeping dynamic topology in mind and all
The possible security issues raised in the security protocol design of the mobile adhoc network. The proposed system provides a fair secure routing model in which malicious nodes in infected routes are stimulated to help forward bundles with secure protocols. In the proposed model, in order to achieve routing security, if and only if the bundles arrive at the destination node, the intermediate forwarding nodes can get acknowledged from the source node. Furthermore, for the failure of bundle forwarding, those intermediate forwarding nodes still can get good acknowledgement values from a trusted authority. Therefore, with this stimulation, the packet delivery performance of MANET can be improved. Moreover, in order to guarantee the feasibility of the fair secure routing model, the proposed system a verifiably encrypted signature technique to provide authentication and integrity protection. In order to prevent the overall performance degradation, i.e., low delivery ratio and high average delay, due to the malicious nodes in infected routes in MANET, the hop-to-hop based secure routing and packet forwarding scheme is adopted. The basic strategy is to provide acknowledgement for intermediate forwarding nodes to faithfully forward packet.

Generally, the intermediate nodes will get acknowledged for packet forwarding from the other nodes, and will take the same mechanism to acknowledge for their packet forwarding requests, by which the overall performance (i.e., high delivery ratio and low average delay) of the MANET can be assured. In the acknowledgement of node-to-node interaction phase if a packet is really relayed to the destination node, the source node will update the acknowledged routes to those intermediate nodes for
Packet forwarding fails to reach the destination node, the source node won’t acknowledge any nodes. Therefore, it is fair to the source node. For the intermediate nodes, although they can’t get better update points for their forwarding in case they still can increase their good reputation values from the trusted authority.

When the gaining factor is large, those intermediate nodes still feel fair for packet forwarding. In addition, since the provably secure short signature schemes are employed, the authentications from the signatures can provide strong witnesses. If an intermediate node didn’t participate in forwarding, it can’t get any acknowledged points. Therefore, from the above analysis, the proposed hop-to-hop secure routing scheme can provide fair security to the Mobile adhoc network. However, the updates are highly encrypted using public key from sender and private keys from destination node.
Figure 4.1 Schematic Illustration of Proposed Model
In this section, we formalize the network model, the node model, and identify the design goal.

A. Network Model

Opportunistic networks are typically characterized by the unguaranteed connectivity and the low frequency of encounters between a given pair of nodes within the network (Fall, 2003). In our model, we consider an opportunistic network as a directed graph $G = (V, E)$, where $V$ and $E$ represent the set of opportunistic network nodes and opportunistic contact edges, respectively. In the opportunistic network, a source $S$ can deliver packets to a destination $D$ via the movement of opportunistic network nodes with proper data forwarding algorithm. Currently, contingent upon whether they allow multiple copies of a message relaying within the network, the existing data forwarding algorithms may be categorized into single-copy and multi-copy algorithms. In the single-copy algorithm (Spyropoulos, 2008), only one copy is relayed in the network until it arrives at the destination. While in the multi-copy algorithms, such as flooding or spray routing (Spyropoulos, 2008), more than one copy are relayed in the networks. Due to large number of message copies in the networks, this kind of approach consumes a high amount of resources which are scarce in opportunistic networks. In this work, in order to clearly illustrate the practical enticement, we just consider a single-copy data forwarding algorithm, i.e., for each bundle $B$, only one copy is initially spread by the source $S$, then the only
copy is opportunistically relayed from one forwarding node to another until its reaching the destination D.

B. Node Model

In opportunistic networks, the selfish behaviors of opportunistic network nodes are naturally caused by human entities that control them (Burgess, 2008) (Chaintreau, 2006). In our model, in order to study the selfish opportunistic network nodes in a non-abstract fashion, we take vehicular ad hoc network as a concrete delay tolerant network of vehicular opportunistic network, where each opportunistic network node is instantiated by vehicle driven by people running in a city environment with some velocity. In the rest of this chapter, we will use the terms "node" and "vehicle" interchangeably to refer to the same opportunistic network entity. In vehicular opportunistic networks, each vehicle is equipped with On Board Unit communication device, which allows different vehicles to communicate with each other based on the 802.11p protocol (Lu, 2008). Note that the 802.11p physical layer offers different bitrates, ranging from 3 to 27 Mbps, from which OBU devices can choose (Shankar, 2006). Therefore, when two vehicles are within the transmission range, e.g., 300 meters, they can exchange bundles (Shankar, 2006). In general, a vehicle is almost resource unlimited, while the equipped OBU communication device is considered resource-constrained, i.e., buffer and computation power constraints (Studer, 2008).

Therefore, there may exists many selfish opportunistic network nodes in the networks. In order to conserve buffer space, these selfish opportunistic network nodes may be very reluctant in the cooperation that is not directly beneficial to them. As a result, the selfishness would be against the goal of the vehicular opportunistic
Secure and Reliable Routing Protocol Design for Mitigating Attacks in MANET

JRN, Rajasthan Vidyapeeth (Deemed) University, Udaipur (Raj.)

Therefore, the cooperation probability of a selfish opportunistic network node can be modeled as follows.

\[ P_c = \mu P_s + (1 - \mu) P_u = \mu P_s + 1 - \mu \]  

(1)

where \( 0 \leq \mu \leq 1 \) is the selfish factor, \( P_s < 1 \) is the cooperation probability under selfish condition, i.e., \( P_s = 0.01 \), while \( P_s = 1 \) denotes the unselfish cooperation probability. Clearly, if \( \mu = 0 \), an opportunistic network node is unselfish, i.e., it is always willing to help with forwarding with probability \( P_c = 1 \). On the contrary, if \( \mu = 1 \), the opportunistic network node is selfish, the cooperation probability is just \( P_c = P_s = 0.01 \). Therefore, the smaller the selfish factor \( \mu \) the better the cooperation in opportunistic networks.

C. Design Goal

Our design goal is to develop a practical enticement protocol to stimulate the selfish opportunistic network nodes to improve the cooperation probability \( P_c \) in the networks. Specifically, the following two desirable objectives will be achieved.

- Improving opportunistic network's performance with stimulation: In order to prevent the overall performance degradation, i.e., low delivery ratio and high average delay, due to the selfish opportunistic network nodes in opportunistic networks, the credit-based enticement strategy is adopted. Similar to (Zhu, 2009), the basic strategy is to provide enticements for intermediate forwarding opportunistic network nodes to faithfully forward bundles. Generally, the intermediate nodes will get paid for bundle forwarding from the other nodes,
payment mechanism to pay for their bundle forwarding requests, by which the overall performance (i.e., high delivery ratio and low average delay) of the opportunistic networks can be assured.

- **Fairness**: In the practical enticement protocol, the fairness is also considered. Concretely, the intermediate forwarding opportunistic network nodes can receive credits if and only if the destination node receives the bundles, which is fair to the source node. At the same time, even though the bundles don’t arrive at the destination, those intermediate opportunistic network nodes who participated in relaying still can get good reputation values for their co-operations. Because a good reputation can build other opportunistic network nodes’ confidence in helping forward the bundles (when the reputation value is higher than a reputation threshold $R_{th}$), the fairness can further stimulate opportunistic network nodes to improve the opportunistic network’s packet delivery performance.

1) **Enticement Strategy**: To achieve the above objectives, the following hybrid enticement strategy is adopted.

- There exists a trusted authority (TA) in the system similar to [20]. Although it does not participate in bundle forwarding in opportunistic networks, TA performs trusted fair credit and reputation clearance for opportunistic network nodes. Therefore, before joining the opportunistic networks, each opportunistic network node should register itself to the TA and obtain its
(PCA) and personal reputation account (PRA) in the initialization phase. Later, when an opportunistic network node has an available fast connection to the TA, it can report to the TA for credit and/or reputation clearance (Zhong, 2003). For example, in the vehicular opportunistic network, a vehicle can communicate with TA for clearance when it makes contact with some Road Side Units (RSUs). For each opportunistic network node, PCA stores its credits, while PRA records its dynamic reputation value as follows: Let $R_{IP(n-1)}$ be the opportunistic network node’s reputation value at time $T_{n-1}$. Then, the new reputation value $R_{IP(n)}$ at time $T_n$ is formulated as $R_{IP(n)} = e^{-\lambda T_i} \cdot R_{IP(n-1)} + C_{T_i}$, where $T_i = T_n - T_{n-1}$, $\lambda$ is the rate at which the reputation value would decrease, and $C_{T_i}$ denotes the reputation cumulative function, which is the summation of new gained reputation values in the time period $T_i$.

- It is not mandatory for the intermediate opportunistic network node to forward bundles. All intermediate nodes in the opportunistic network can self-determine whether or not to participate in bundle forwarding.

- However, once an intermediate opportunistic network node participates in forwarding bundle, it can get the credits from the source node as well as reputation values from the TA.
If the bundle doesn’t arrive at the destination node, the source node won’t need to pay credits. However, those intermediate nodes who helped forward can still get good reputation values from the TA. Based on the above reputation calculation, if no new reputation value is gained in $T_i$, i.e., $C_{Ti} = 0$, then $R_{IP(n)} = e^{-\lambda T_i} \cdot R_{IP(n-1)}$ will decrease with the time. The larger the parameter $\lambda$, the quicker the reputation value $R_{IP(n)}$ decreases. Therefore, in order to keep/increase good reputation values, this fair enticement strategy are attractive to each opportunistic network node.

The design of reward calculation is the pivot of a practical enticement protocol, which should guide the selfish opportunistic network nodes to follow the protocol to help with forwarding bundles. In the enticement model, the following reward calculation is exercised: once an intermediate opportunistic network node $N_i$ helped forward a bundle for $D_{isi}$ distance, it can get a reward either $D_{isi} \cdot C_{IP} + D_{isi} \cdot R_{IP}$ if the bundle $B$ arrives at the destination $D$ finally or $D_{isi} \cdot R_{IP}$ otherwise, i.e.

\[
\text{Reward}_i = \begin{cases} 
D_{isi} \cdot C_{IP} + D_{isi} \cdot R_{IP}, & \text{if } B \text{ arrives at } D \\
D_{isi} \cdot R_{IP}, & \text{otherwise}
\end{cases}
\]

(2)

where $C_{IP}$ is a unit enticement credit provided by the source $S$, $R_{IP}$ is a fixed unit reputation value defined by the TA for optimizing the network. Assume that $C_F$ is the unit resource cost used for forwarding. We define the gaining factor of opportunistic network node $N_i$ as.
and redefine the cooperation probability of Ni with reputation value $R_{IP}$ as

$$P_c = \begin{cases} 
1 & \text{if } R_{IP} < R_{th} \\
1 & \text{elseif } R_{IP} \geq R_{th} \\
(\alpha_i - \zeta_i)P + 1 - (\alpha_i - \zeta_i) & \alpha_i - \zeta_i > 0
\end{cases}$$

Then, with the cooperation probability $P_c$, the opportunistic network node $N_i$ is interested in helping forward the bundle. Note that, when $R_{IP} \geq R_{th}$, different intermediate opportunistic network node may have different initial selfish factor $\bar{U}_i$. Therefore, to guarantee the success of stimulation on all intermediate opportunistic network nodes, the source $S$ can choose a large $C_{IP}$ (i.e., large gaining factor $\zeta$) in its enticement policy such that each $\bar{U} - \zeta$ can be minimal. In addition, since $\text{Reward}_i$ is a linear increase function of $D_{isi}$ in Eq. (2), the longer the $D_{isi}$, the more the $\text{Reward}_i$. Therefore, the intermediate node is willing to forward the bundle as long as possible.

### 4.4 PROPOSED ENTICEMENT PROTOCOL

In this section, we propose protocol that consists of four parts: system initialization, bundle generation, bundle forwarding, and charging and rewarding. Before describing them, we first review the bilinear pairing technique (Boneh, 2001), which is a mature cryptographic technique and serves as the basis of the proposed protocol.

**A. Bilinear Pairing**

1. Design for Mitigating Attacks in MANET
Let $G, G^T$ be two multiplicative cyclic groups of the same prime order $q$. Suppose $G$ and $G^T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : G \times G \rightarrow G^T$ such that $e(g_1^a, g_2^b) = e(g_1^a, g_2^b)^{ab} \in G^T$ for all $a, b \in \mathbb{Z}_q^*$ and any $g_1, g_2 \in G$ [28]. In group $G$, the Computational Diffie-Hellman (CDH) problem is considered to be hard, i.e., given $(g, g^a, g^b)$ for $g \in G$ and unknown $a, b \in \mathbb{Z}_q^*$, there is no algorithm running in expected polynomial time, which can compute $g^{ab}$ with non-negligible probability, while the Decisional Diffie-Hellman (DDH) problem is easy, i.e., given $(g, g^a, g^b, g^c)$ for $g \in G$ and unknown $a, b, c \in \mathbb{Z}_q^*$, it is easy to judge whether $c = ab \mod q$ by checking $e(g^a, g^b) = e(g^c, P)$.

Definition 1: A bilinear parameter generator $G_{\text{gen}}$ is a probabilistic algorithm that takes a security parameter $k$ as input, and outputs a 5-tuple $(q, g, G, G^T, e)$ where $q$ is a $k$-bit prime number, $G, G^T$ are two groups with order $q$, $g \in G$ is a generator, and $e : G \times G \rightarrow G^T$ is a non-degenerated and efficiently computable bilinear map.

B. The Protocol Design

1) System Initialization: We assume that all opportunistic network nodes $N = \{N_1, N_2, \ldots\}$ and TA are using the same suite of system parameters. Given the security parameter $k$, the bilinear parameters $(q, g, G, G^T, e)$ are first generated by running $G_{\text{gen}}(k)$. Then, a cryptographic hash function $H : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ and a secure symmetric encryption algorithm $\mathcal{E}()$ are chosen [28]. In the end, the system parameter $\text{params} = (q, g, G, G^T, e, H, \mathcal{E})$ are published.
Each opportunistic network node with a unique identity \( N_i \in N \) chooses a random number \( x_i \in \mathbb{Z}_q^* \) as its private key and computes the corresponding public key as \( y_i = g^{x_i} \). At the same time, each opportunistic network node \( N_i \in N \) also registers its personal credit account (PCA) and personal reputation account (PRA) to the TA. Note that, all public keys in the system should be certified by public key certificates issued by certificate authority (CA). In addition, each opportunistic network node\'s reputation value \( R_{IP} \) during a period is signed by TA and anyone can check it.

2) Bundle Generation: When a source node \( S \) with the private-public key pair \( (x_s, y_s = g^{x_s}) \) at location \( L_s \) wants to send a bundle \( m \) to the destination node \( D \) with the key pair \( (x_d, y_d = g^{x_d}) \) at location \( L_d \), \( S \) will run the following steps.

Step 1. Compute the static shared key \( K_{sd} = y_d^{x_s} = g^{x_s x_d} \) between \( S \) and \( D \), and encrypt the bundle \( m \) into \( B = \mathcal{E}_{K_{sd}}(m) \) to achieve confidentiality.

Step 2. Determine a proper enticement policy (IP) as in Eq. (2), and make a verifiably encrypted signature \( \hat{\sigma}_0 \) on \( M_0 = S \mid L_s \mid D \mid L_d \mid IP \mid TTL \) and \( B \) as

\[
\sigma_0 = y_d^{(H(M_0||B)+x_s)^{-1}}
\]

When an intermediate node \( N_1 \) is interested in the IP and willing to forward the bundle to a possible location \( L_1 \), it first checks the source\'s reputation value \( R_{IP} \) and verifies the validity of \( \hat{\sigma}_0 \) with the equation

\[
e(\sigma_0, g^{H(M_0||B)})^? = e(y_d, g)
\]
If the source's reputation is acceptable, i.e., $R_{IP} \geq R_{th}$, and the equation holds, $N_1$ signs

$$\sigma_1^* = g^{(h(M_o || N_1 || L_s || TS) + x_1)}$$

as an Interest Acknowledgement (ACK), and sends $\hat{u}_1^*$ and $L_1$ to the source node $S$. After receiving $\hat{u}_1^*$ and $L_1$, the source node $S$ runs the next steps.

Step 3: Verify the validity of ACK by checking the equation

$$e(\sigma_1^*, g^{h(M_o || N_1 || L_s || TS) \cdot y_1}) = e(g, g)$$

If it holds, $S$ makes the signature $\hat{u}_1$ on $M_o || N_1 || L_s || TS$ as

$$\sigma_1^* = g^{(h(M_o || N_1 || L_s || TS) + x_s)}$$

Otherwise, $S$ neglects the ACK.

Step 4. Set the base layer as $BL = (M_o || \hat{u}_1 || N_1 || L_s || TS || \hat{u}_1)$ and forward the bundle $B$ together with the base layer $BL$ to the intermediate node $N_1$ as follows

$$S \rightarrow N_1: B, BL$$

After verifying

$$\sigma_1^* = g^{(h(M_o || N_1 || L_s || TS) + x_s)}$$

by checking,

$$e(\sigma_1^*, g^{h(M_o || N_1 || L_s || TS) \cdot y_s}) = e(g, g).$$

$N_1$ begins to forward the bundle.

When approaching to the location $L_1$, the intermediate node $N_1$ considers it cannot carry the bundle $B$ close to the destination node $D$ anymore and forwards the bundle to the next-hop opportunistic network node by running the Algorithm 1. Likewise,
Without loss of generality, the bundle B finally arrives at the destination node D by opportunistic bundle forwarding with the routing $S \rightarrow N_1 \rightarrow N_2 \rightarrow \cdots \rightarrow N_1 \rightarrow D$.

In the following, the detailed bundle forwarding protocol is described.

### 4.5 ALGORITHM EXECUTION

The proposed system is simulated on standard 32 bit Windows OS on Java Platform. Computer simulation is one of the most widely used way to evaluate the MANET routing protocols. Because it provides four main advantages (i) it enables experimentation with large networks; (ii) it enables experiments with configurations that may not be possible with existing technology; (iii) it allows for rapid prototyping by significantly abstracting the complexity of the real system. Simulators enable the development and debugging of new protocols with reduced effort and (iv) it makes reproducible experiments in a controlled environment possible. The working of Secure Routing Protocol in MANET is explained is that messages in ad hoc network must be authenticated to guarantee the integrity and non-repudiation so that the protocol and nodes can be prevented against several kinds of attacks.

**Key Agreement Process between Neighbor Nodes:** A node joining a network requires sending key agreement messages to its neighbors to negotiate a shared secret key.

**Algorithm 1:** For node-to-node authentication of the Network Model

1. Begin
2. Input: Set of number of nodes
4. Sender node broadcasts a message indicating the negotiation request with neighbor nodes
5. "Key_agreement_req, request_id, sender_address, PK_S"
6. Sender node gets reply a message
7. "Key_agreement_rep, request_id, sender_address, neighbor_address, PK_N"
8. Generate a key Ks by using a secure random number generator,
9. Encrypt Ks with PKB (node B's public key) = encrypt PKB (Ks),
10. Send an offer message
11. "KEY_PASS, encrypt PKB (Ks)" to B,
12. Wait ACK (acknowledgement) from B and check message integrity to finish the negotiation
13. Let node B receives the key passing message; it decrypts "encrypt PKB (Ks)" by its private key (pB) to get the shared key K. Then, node B sends the ACK message
14. "KEY_PASS_ACK, request_id, HASH_Ks (request_id)"
15. successful shared secret key negotiation,
16. END

Where PK_S and PK_N is the public key of the sender node and replying node, each node in a network has its own a pair of public key e and private key d following RSA Public-key Crypto-system by self-generation, and each node contains a list of neighbor nodes with records containing the information of a neighbor node including neighbor address, neighbor public key, and a shared secret key. This information is formed after the key agreement between two neighbor nodes to negotiate a pair of keys and a shared secret key.
Secure and Reliable Routing Protocol Design for Mitigating Attacks in MANET

Route Request: Route request (RREQ) is initiated by a source node (S) and then propagated by intermediate nodes until the message reaches its destination node (D).

Algorithm 2: Identification of the required bundle signature

1. Begin
2. Input: Set of number of bundle
3. Output: Identification of the required destination node and path to simulation the required bundle signature
4. Initialize the nodes, speed, radio range and bundle status
5. Get Encrypted bundle in array list
6. Set encrypted bundle in binary
7. Choose and get initial Personal credit account
8. Choose and set initial personal reputation account
9. Generate the create bundle
10. For {
    a. Determine the no. of bundle values
    b. Evaluate each signature of the nodes
    c. }
11. Generate the receive bundle
12. For {
    a. Unique id of the nodes
    b. Add the authorized nodes
    c. Remove the unauthorized nodes
    d. }
13. Generate the forwarded bundle
14. Trusted authority has forwarded from sender node to receive nodes
15. if (Current Time <= Received time + Holding time) then
    a. {
        i. Forwarded Bundle to receive nodes
b. Else
   i. {
      1. If (encrypted bundle = null) then
      2. {Set the bundle status
      3. }
   }
16. Return bundle status
17. END

4.6 SUMMARY

This chapter discusses about the proposed model that was evaluated on advance application of mobile adhoc network considering the presence of vehicles nodes in the opportunistic network of MANET that poses higher dimensionality of the threats.

The accomplished results from this model is discussed in next chapter.