Dynamic Segmented Network Coding Scheme for Bulk Data Distribution in Delay Tolerant Networks

AR.Umayal¹, K.Tamilselvan²
¹Pg Scholar,²Assistant Professor
¹²Computer Science, A.V.C College of Engineering, Mayiladuthurai, Tamil Nadu.

Abstract-Delay Tolerant Networks(DTNs)have been identified as one of the key areas in the field of wireless communications. They are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. DTNs attempt to route network messages via intermittently connected nodes. We propose a network architecture and application interface structured around optionally-reliable asynchronous message forwarding, with limited expectations of end-to-end connectivity and node resources. The architecture operates as an overlay above the transport layers of the network it interconnects, and provides key services such as network data storage and retransmission, interoperable naming, authenticated forwarding and a coarse-grained class of service. Epidemic routing using random linear network coding has been studied and proved as an efficient way for delivering small amount of data. We address dynamic trust management, i.e., determining and applying the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance.

Key terms: Delay Tolerant Networks, dynamic trust management, secure routing, performance analysis/evaluation.

I.INTRODUCTION

Delay tolerant network (DTN) comprises mobile nodes (e.g., humans in a social DTN) experiencing sparse connection, opportunistic communication, and frequently changing network topology. Because of lack of end-to-end connectivity, routing in DTN adopts a store-and-forward scheme by which messages are forwarded through a number of intermediate nodes leveraging opportunistic encountering, hence resulting in high-end-to-end latency. Epidemic routing has been extensively investigated in the literature. Epidemic routing is flooding-based in nature, where the “store and forward” approach is adopted. propose dynamic trust management for DTNs to deal with both malicious and selfish misbehaving nodes. Our notion of selfishness is social selfishness as very often humans carrying communication devices (smart phones, GPSs, etc.) in a DTN are socially selfish to outsiders but unselfish to friends. Our notion of maliciousness refers to malicious nodes performing trust-related attacks to disrupt DTN operations built on trust. We aim to design and validate a dynamic trust management protocol for DTN routing performance optimization in response to dynamically changing conditions such as the population of misbehaving nodes.

The contributions of the paper relative to existing work in trust/reputation management for DTNs are summarized as follows.

1. We propose to combine social trust deriving from social networks and traditional quality of service (QoS) trust deriving from communication networks into a composite trust metric to assess the trust of a node in a DTN. To cope with both malicious and socially selfish nodes, we consider “healthiness” and “unselfishness” as two social trust metrics.

2. We propose the notions of “subjective trust” versus “objective trust” based on ground truth for protocol validation. For example, the healthiness trust of a good node should converge to 1 (ground truth) minus a false positive probability caused by noise, while the healthiness of a bad node should converge to 0 (ground truth) plus a false negative probability caused by noise and the random attack probability with which this bad node performs trust-related attacks.

3. We address the issue of application performance maximization through dynamic trust management by adjusting trust aggregation/formation protocol settings dynamically in response to changing conditions to maximize DTN routing performance. Essentially we address the importance of integration of trust and security metrics into routing and replication decisions in DTNs.

4. We develop a novel model-based methodology utilizing stochastic petri net (SPN) techniques for the analysis of our trust protocol and validate it via extensive simulation. The model validated with simulation yields actual ground truth node status against which “subjective” trust obtained from executing the trust protocol is verified, and helps identify the best protocol settings in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance.
5. We perform a comparative analysis of our trust-based DTN routing protocol built on top of dynamic trust management with simulation validation against routing based on Bayesian trust management (called Bayesian trust-based routing for short) and non-trust-based (PROPHET and epidemic) protocols. Our trust-based routing protocol outperforms Bayesian trust-based routing and PROPHET. Further, it approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

We validate our trust management protocol design through extensive simulation using both synthetic and real mobility data. demonstrate the effectiveness of (DTM).

II. SYSTEM MODEL

We consider a DTN environment with no centralized trusted authority. Nodes communicate through multiple hops. When a node encounters another node, they exchange encounter histories certified by encounter tickets so as to prevent black hole attacks to DTN routing. We differentiate socially selfish nodes from malicious nodes. A selfish node acts for its own interests including interests to its friends, groups, or communities. So it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the source, current carrier or destination node. We consider a friendship matrix to represent the social ties among nodes. Each node keeps a friend list in its local storage. A similar concept to the friendship relationship is proposed in where familiar strangers are identified based on colocation information in urban transport environments for media sharing. Our work is different from in that rather than by frequent colocation instances, friendship is established by the existence of common friends. Energy spent for maintaining friend lists and executing matching operations is negligible because energy spent for computation is very small compared with that for DTN communication and matching operations are performed only when there is a change to the friend list. When a node becomes selfish, it will only forward messages when it is a friend of the source, current carrier, or the destination node, while a well-behaved node performs altruistically regardless of the social ties. A malicious node aims to break the basic DTN routing functionality. In addition to dropping packets, a malicious node can perform the following trust-related attacks:

1. Self-promoting attacks: it can promote its importance (by providing good recommendations for itself) so as to attract packets routing through it (and being dropped).
2. Bad-mouthing attacks: it can ruin the reputation of well-behaved nodes so as to decrease the chance of packets routing through good nodes.
3. Ballot stuffing: it can boost the reputation of bad nodes (by providing good recommendations for them) so as to increase the chance of packets routing through malicious nodes (and being dropped).

III. TRUST MANAGEMENT PROTOCOL

Our trust protocol considers trust composition, aggregation, formation and application-level trust optimization design. Fig.1 Ballot stuffing and bad-mouthing attacks are a form of collaborative attacks to the trust system to boost the reputation of malicious nodes and to ruin the reputation of (and thus to victimize) good nodes. Mitigate collaborative attacks with an application-level trust optimization design by setting a trust recommender threshold $T_{rec}$ to filter out less trustworthy recommenders, and a trust carrier threshold $T_{c}$ to select trustworthy carriers for message forwarding.

![Fig. 1. A flowchart for trust protocol execution.](image)

We consider two types of trust properties:

1. QoS trust: QoS trust is evaluated through the communication network by the capability of a node to deliver messages to the destination node. We consider “connectivity” and “energy” to measure the QoS trust level of a node. The connectivity QoS trusts about the ability of a node to encounter other nodes due to its movement patterns. The energy
QoStrust is about the battery energy of a node to perform the basic routing function.

2. Social trust: Social trust is based on honesty or integrity in social relationships and friendship in social ties. We consider “healthiness” and social “unselfishness” to measure the social trust level of a node. The healthiness social trust is the belief of whether a node is malicious. The unselfishness social trust is the belief of whether a node is socially selfish. While social ties cover more than just friendship, we consider friendship as a major factor for determining a node’s socially selfish behavior.

The selection of trust properties is application driven. In DTN routing, message delivery ratio and message delay are two important factors. We consider “healthiness”, “unselfishness”, and “energy” in order to achieve high message delivery ratio, and we consider “connectivity” to achieve low message delay.

We define a node’s trust level as a real number in the range of [0, 1], with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust. We consider a trust formation design (described in the middle part of Fig. 1) by which the trust value of node $i$ evaluated by node $j$ at time $t$, denoted as $T_{ij}(t)$, is computed by a weighted average of healthiness, unselfishness, connectivity, and energy as follows:

$$T_{ij}(t) = \sum_{x} w^x \times T_{ij}^x(t),$$

A collaborative attack means that the malicious nodes in the system boost their allies and focus on particular victims in the system to victimize.

**IV. PROPOSED SYSTEM**

The main aim is to identify the best weight ratio under which the application performance (secure routing) is maximized, given an operational profile as an input. DTM (Dynamic Trust Management) deals with selfish and malicious nodes DTN (Delay Tolerant Networks) for secure routing. Design and validate a dynamic trust management protocol for delay tolerant network routing performance optimization in response to dynamically changing conditions such as the population of misbehaving nodes.

Trust protocol evaluates trust composition, trust aggregation, trust formation, and application-level trust optimization designs. Proposed system to combine social trust deriving from social networks and traditional quality of service (QoS) trust deriving from communication networks into a composite trust metric to assess the trust of a node in a DTN. The notions of “subjective trust” versus “objective trust” based on ground truth for protocol validation. Methodology utilizing “Stochastic Petri Net” (SPN) techniques for the analysis of our trust protocol and validate it via extensive simulation.
Main advantage is it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the source, current carrier or destination node. Delay tolerant networks bundle of packets and send source to destination.

Trust protocol considers:
- Trust Composition,
- Trust Aggregation,
- Trust Formation.

Our notion of social selfishness is that friends will be cooperative toward each other even if they are selfish. Every node keeps a friend list and also adds itself as a member. When node i and node j encounter and directly interact with each other, if there is a change to either friend list, they can exchange their friend lists. To preserve privacy, node i and node j can agree on a one-way hash function (with a session key) upon encountering while exchanging the friend lists to hide the identities of their friends. This way, only common friends (the source node, node i, node j, or the destination node) will be identified while the identities of uncommon friends will not be revealed.

We validate our trust management designs by a novel model-based analysis methodology via extensive simulation. Specifically we develop a mathematical model based on continuous-time semi-Markov stochastic processes (for which the event time may follow any general distribution) to define a DTN consisting of a large number of mobile nodes exhibiting heterogeneous social and QoS behaviours.

We develop a probability model based on stochastic petri net techniques to describe a DTN, given an operational profile as input. The SPN model for a DTN node is shown in consisting of four places, namely, energy, location, maliciousness and selfishness. The underlying state machine is a semi-Markov model with 4-component states, i.e.,(energy, location, maliciousness, selfishness), where energy is an integer holding the amount of energy left in the node, location is an integer holding the location of the node, maliciousness is a binary variable with 1 indicating the node is malicious and 0 otherwise, and selfishness is a binary variable with 1 indicating the node is socially selfish and 0 otherwise. A selfish node will forward a packet only if the source, current carrier or the destination is in its friend list. Here we note that a node’s trust value actually is a real number in [0, 1]; it is calculated by a state-probability weighed sum of trust values assigned to the states of the underlying semi-Markov model of the SPN performance model, i.e., trust value ¼ Pi (state probability of state i _trust value in state i). In some states, the trust value is binary. For example in a state in which a node is compromised, the trust value for property “healthiness” in this state is 0. Note that each node has its own SPN model. So there are as many SPN models as they are nodes in the DTN. The operational profile specifies the percent of malicious nodes and the percent of socially selfish nodes. Thus, some nodes will be malicious in accordance with this specification. Similarly some nodes will be selfish based on the percent of selfish nodes. The purpose of the SPN model is to yield ground truth status of a node in terms of its healthiness, unselfishness, connectivity, and energy status. Then we can check subjective trust against ground truth status for validation of trust protocol designs. Below we explain how we leverage the SPN model to determine a node’s ground truth status.

Location (Connectivity): The connectivity trust of node mtoward node d is measured by the probability that both node m and node d are in the same location at time t. We use the location subnet to describe the location status of a node. Transition T_LOCATION is triggered when the node moves to a new area from its current location according to its mobility pattern. We consider both synthetic mobility models based on SWIM and real mobility traces. This information along with the location information of other nodes at time t provides us the probability of two nodes encountering with each other at any time t.

Healthiness: A malicious node is necessarily unhealthy. So we will know the ground truth status of healthiness of the node by simply inspecting if place maliciousness contains a token.

Unselfishness: A socially selfish node drops packets unless the source, current carrier or the destination node is in its friend list. We will know the ground truth status of unselfishness of the node by simply inspecting if place selfishness contains a token.

Dynamically changing environment conditions: With the goal to deal with malicious and selfish nodes in DTN routing, in this paper we consider a dynamically changing environment in which the number of misbehaving nodes (malicious or selfish) is changing over time.

V. IMPLEMENTATION

5.1 Channel available checking module:

First checking the path is available or not? Among Multiple Path we are going to choose the nearest path. That Nearest path should be safe without any packet loss. After Receive the acknowledgement alone, we will send the full packets. Instead of sending full message to destination. It will empty message or simple data for checking process while getting ACK after that only send full packets/data. It will save time and cost, because in between any packet loss mean its waste of cost. In terms of robustness against attacks in a
realistic DTN environment. Further, the proposed algorithm is very efficient in terms of its computational complexity. Whenever a source node sends some packets belonging to the flow that is initiated by itself, it creates a bloom filter from those packets. We analytically obtained the waiting time of a judge node before executing and evaluated the effects of attacks on the detection scheme for a network of size $N$ in which the inter-contact time between two particular nodes.

5.2 Dynamic trust management process module

Nodes communicate through multiple hops. When a node encounters another node, they exchange encounter histories certified by encounter tickets so as to prevent black hole attacks to DTN routing. We differentiate socially selfish nodes from malicious nodes. A selfish node acts for its own interests including interests to its friends, groups, or communities. So it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the source, current carrier or destination node.

5.3 Secure Routing module

When the network connections are dropped that time enable the Secure Router and catch the dropped nodes dynamically immediate. Design and validate a Router when secure routing performance optimization in response to dynamically changing conditions such as the population of misbehaving nodes. In addition to dropping packets, a malicious node can perform the following trust-related attacks. Dynamic trust management adjusting trust aggregation/formation protocol settings dynamically in response to changing conditions to maximize DTN Routing performance.

5.4 Adjust and Update Trust Level

In DTN routing, message delivery ratio and message delay are two important factors. We consider “healthiness”, “unselﬁshness”, and “energy” in order to achieve high message delivery ratio, and we consider “connectivity” to achieve low message delay so develop the trust management protocol algorithm for enabled DTN Networks. Delay tolerant networks (DTNs) are basically by high end-to-end latency, frequent disconnection, and opportunistic communication over untrustworthy wireless links so adjust and update the nodes dynamically. Our trust protocol considers trust composition, trust aggregation, trust formation and application-level trust optimization designs Social trust: Social trust is based on honesty or integrity in social relationships and friendship in social ties.
VI. CONCLUSION

Trust management protocol for DTNs and useful it to secure routing shows its utility. Trust management protocol combines QoS trust with social trust to obtain a composite trust metric. Design allows the best trust setting for trust aggregation to be identified so that subjective trust is closest to objective trust for each individual trust property for minimizing trust bias. Design also allows the best trust configuration to be identified to make best use of application presentation. Established how the results obtained at design time can facilitate dynamic trust management for DTN routing in response to dynamically changing conditions at runtime.

VII. REFERENCES


