OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Hierarchical Trust Management for Delay Tolerant Networks Using Stochastic Petrinet for Secure Routing

Chithra M.[1], Mr. Vimalathithan M. E.[2],
[1, 2] *(PG scholar, Professor, Department of Computer science and Engineering Indra Ganesan College of Engineering Trichy-12, TamilNadu)*

Abstract: *A highly scalable trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. Delay tolerant networks (DTNs) are characterized by high end-to-end latency, frequent disconnection, and opportunistic communication over unreliable wireless links.. But this suffers from buffer space limitation. Thus, to achieve efficient utilization of network resources, it is important to come up with an new message scheduling strategy to determine which messages should be forwarded and which should be dropped in case of buffer is full. A novel message scheduling framework for epidemic and two-hop forwarding routing maintains the forwarding or dropping decision. It checks for the nodes priority for message delivery. This can be made at a node during each contact to achieve optimal message delivery ratio or message delivery delay and also buffer space is maintained. The experimental result shows that the proposed message scheduling framework can achieve better performance.*

Index terms: *Secure Routing, performance analysis, Design and validation, DTN.*

I. Introduction

He characteristics of a delay tolerant network is the lack of Tan end-to-end path for a given node pair for an extended period. The novelty and challenges inherent in DTN routing, the implementation includes a custom internal interface to the route selection and message forwarding components that eases development of new algorithms. The Internet architecture has proven to be an unparalleled success in its ability to provide network connectivity that spans the globe. However, some of the not necessarily explicit assumptions of the Internet architecture do not hold in many environments. Examples of these situations include mobile and ad-hoc networks, wireless sensor networks, deep-space communication, and some deployments in developing regions with limited power and telecommunications infrastructure. Epidemic routing is flooding-based in nature, as nodes continuously replicate and transmit messages to newly discovered contacts that do not already possess a copy of the message; the epidemic protocols require multicasting of bundles in response to opportunistic contacts where utility of the peers that are encountered decays with time.

Thus it maintains the secure routing and also reduces message delivery delay as well as it increases the message delivery ratio. It deals with the message propagation prediction under epidemic forwarding and evaluates the delivery delay and or delivery ratio at any time instance during message lifetime. This paper is organized as follows: Section II Presents Related Work. Section III presents proposed Techniques. The Experimental Results of the schemes are presented in section IV Section V presents conclusion of this paper.

II. Related Work

Secure Routing for Partially Connected Ad Hoc Networks [A. Vahdat and D. Becker, Technical Report CS- 200006, Duke Univ., Apr. 2000].Mobile ad hoc routing protocols allow nodes with wireless adaptors to communicate with one another without any network infrastructure. Existing ad hoc routing protocols, while robust to rapidly changing network topology, assume the presence of a connected path from source to destination. Given power limitations, the advent of short-range wireless networks, and the wide physical conditions over which ad hoc networks must be deployed, in some scenarios it is likely that this assumption is invalid. Techniques to deliver messages in the case where there is never a connected path from source to destination or when a network partition exists at the time a message is originated. Finally epidemic routing is introduced, where random pair-wise exchanges of messages among mobile hosts ensure eventual message delivery. Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case [Spyropoulos, K. Psounis, and C.S. Raghavendra, IEEE Trans. Networking, vol. 16, no. 1, pp. 63-76, Feb. 2008] Intermittently connected mobile networks are wireless networks where most of the time there

does not exit a complete path from the source to the destination. There are many real networks that follow this model, for example, wildlife tracking sensor networks, military networks, vehicular ad hoc networks, etc. Then propose a family of multi-copy protocols called Spray routing, which can achieve both good delays and low transmissions. Spray routing algorithms generate only a small, carefully chosen number of copies to ensure that the total number of transmissions is small and controlled. The proposed security mechanism consists of a trust management mechanism and an iterative reputation management scheme despite this, theory and simulations show that secure routing:

1. To maintain social selfishness, SSAR allocates resources such as buffers and bandwidth based on packet priority which is related to the social relationship among nodes.
2. At the same time achieve better delays than all existing schemes in most scenarios, if carefully designed. It has very desirable scalability characteristics, with its relative performance improving as the network size increases. The Message Delay in Mobile Ad Hoc Networks [R.Groenevelt,p.Nain and G.Koole, July-2005]A stochastic model is introduced that accurately models the message delays in mobile ad hoc networks where nodes relay messages and the networks are sparsely populated. The model has only two input parameters:

1. The number of nodes.
2. Parameter of an exponential distribution which describes the time until two random mobiles come within communication range of one another.

From this we derive both a closed-form expression and an asymptotic approximation of the expected message delay. As an additional result, the probability distribution function is obtained for the number of copies of the message at the time the message is delivered.

These calculations are carried out for two factors:

1. Healthiness. 2. Unselfishness. Routing protocols using relay nodes have been proposed that increase the message delivery ratio in mobile ad hoc networks. These protocols operate on a store-carry-forward mode to take advantage of node mobility to improve node connectivity, and ultimately the message throughput

III. System Overview

Hierarchical trust management using Stochastic Petri Net technique to increase the message delivery ratio also reduces the message delivery delay.

1) NODE FORMATION MODULE

In node formation module, to analyze social relations between nodes (i.e. people), Need to define their neighbor node in terms of their behavior. For this purpose, we define new metric measuring different aspects of neighbor node behavior recorded in the history of their encounters with other nodes. It also differentiates according to time of day and proposes to use different friendship communities in different time periods. Each node keeps a friend list in its local storage. A similar concept to the friendship relationship, where familiar strangers are identified based on co location information in urban transport environments for media sharing.

The goals of Secure Routing are to:

1. Maximize message delivery rate.
2. Minimize message latency.
3. Minimize the resource consumption.

2) ANALYSIS THE TRUST NODE LIST

In this module QoS trust is evaluated through the communication network by the capability of a node to deliver messages to the destination node. Consider connectivity and energy to measure the QoS trust level of a node. The connectivity QoS trust is about the ability of a node to encounter other nodes due to its movement patterns. The energy QoS trust is about the battery energy of a node to perform the basic routing.

3) SPN MODULE

In this SPN module 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. 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.

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.

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 behaviors. We take the concept of operational profiles in software reliability engineering as we build the mathematical model. An operational profile is what the system expects to see during its operational phase. During the testing and debugging phase, a system would be tested with its anticipated operational profile to reveal design faults. Failures are detected and design faults causing system failures are removed to improve the system reliability. The operational profile of a DTN system specifies the operational and environmental conditions. Typically this would include knowledge regarding (a) hostility such as the expected % of misbehaving nodes and if it is evolving the expected rate at which nodes become malicious or selfish or even the expected % of misbehaving nodes as a function of time; (b) mobility traces providing information of how often nodes meet and interact with each other; (c) behavior specifications defining good behavior and misbehavior during protocol execution; and (d) resource information such as how fast energy is consumed.

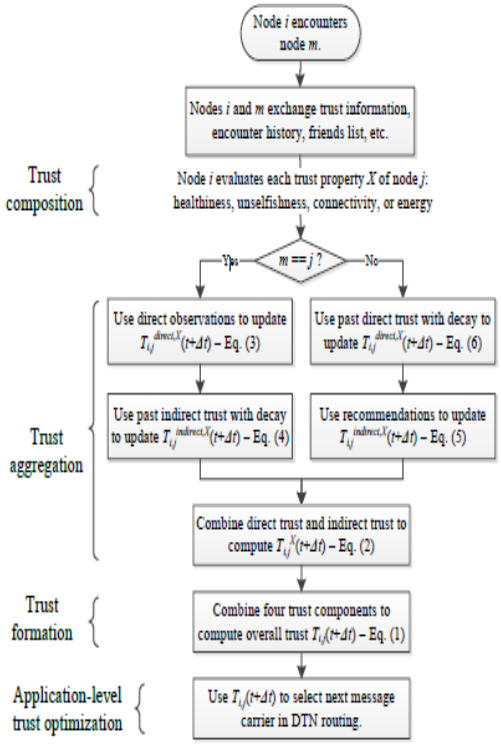


Fig. 1. sy stem architecture.

a. Location (Connectivity): The connectivity trust of node m toward 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.

b. Energy: We use the energy subnet to describe the energy status of a node. Place energy represents the current energy level of a node. An initial energy level ( ) of each node represented by a number of tokens is assigned according to node heterogeneity information. A token is taken out when transition T_ENERGY fires representing the energy consumed during protocol execution, packet forwarding and/or performing attacks in the case of a malicious node. The rate of transition T_ENERGY indicates the energy consumption rate which varies depending on the ground truth status of the node (i.e., malicious or selfish). The operational profile specifies the energy consumption rate of a malicious node vs. a selfish node vs. a well-behaved node.

c. 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.

d. 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.

4) TRUST BASED DTN ROUTING

Trust-based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio. 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 This module is used for the purpose of message scheduling. The message scheduling framework consists of 4 processes.

1. Summary Vector Exchange Module (SVEM):

The network information summarized as a summary vector is exchanged between the sender and the intermediate nodes, which includes the following data:

1) Statistics of inter encounter time of every node pair maintained by the nodes.
2) Statistics regarding the buffered messages, including their IDs, remaining time to live (Ri), destinations for each incoming message.

2. Network State Estimation Module (NSEM):

The NSEM is used to obtain the estimated mi (Ti), ni (Ti), and si (Ti) Where,
mi (Ti) – Number of nodes who have seen message i
ni (Ti) - Number of copies of the message i.
si (Ti) – Number of nodes who have seen message i and their buffers were not full.

3. Utility Calculation Module (UCM):

UCM is used to optimize the average delivery ratio or delivery delay i.e., estimates per- message utility value.

4. Decision:

The decision of forwarding or dropping the buffered messages is made based on the buffer occupancy status and the utility value of the messages.

5) PERFORMANCE EVALUATION

In this Module it compares the message delivery ratio, delay, and overhead generated by our trust protocol against Bayesian trust-based, PROPHET, and epidemic routing protocols. The results demonstrate that our trust-based secure routing protocol designed to maximize delivery ratio can effectively trade off message overhead for a significant gain in delivery ratio. In particular, our protocol and Bayesian trust-based routing have less performance degradation in message delivery ratio than PROPHET when the percentage of malicious nodes increases. The reason is that using trust to select the next message carrier can avoid messages being forwarded to malicious nodes and then being dropped. Further, our trust- based routing protocol outperforms Bayesian trust-based routing and PROPHET in delivery ratio as it applies the best trust formation out of social and QoS trust properties. Moreover, it is assumed that every node is aware of all messages that has encountered during contacts with other nodes, which raises practicability issue. This can be resolved by a newly proposed technique, it will provide optimal message delivery ratio and also reduces the message delivery delay.

RATE (%)	RATE AVG(S)	LATENCY	DELI-VERY
250m	94.0	98.2	100.0
100m	99.0	34.3	100.0
10m	99.0	82.0	97.0
25m	98.0	85.3	99.0

3.1TECHNIQUES USED

1. Best Trust Formation Protocol Settings to Maximize Application Performance

The trust formation issue to optimize application performance. For the secure routing application, two most important performance metrics are message delivery ratio and delay. The delivery ratio as the percentage of messages that are delivered successfully within an application deadline which is the maximum delay the application can tolerate. The best trust formation for maximizing delivery ratio under double- copy forwarding, given the percentage of malicious nodes as input. First observe there is a distinct set of optimal weight

settings under which delivery ratio is maximized. Second, the optimal weight of the healthiness trust property increases as the % of malicious node increases. The maximum delivery ratio obtainable when the system operates under the best trust formation setting identified. The delivery ratio remains high even as the % of malicious nodes increases to as high as 45%. This to some extent demonstrates the resiliency property of our trust-based routing protocol against malicious attacks.

2. Best Application-Level Trust Optimization Design Settings to Maximize Application Performance

An application-level trust optimization design by setting a trust recommender threshold to filter out less trustworthy recommenders, and a trust carrier threshold to select trustworthy carriers for message forwarding .These two thresholds are dynamically changed in response to environment changes. A node's trust value is assessed based on direct trust. The trust of one node toward another node is updated upon encounter events. Each node will execute the trust protocol independently and will perform. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structure of the system which comprises system components, the externally visible properties of those components, the relationships between them and provides a plan from which products can be procured and systems developed that will work together to implement the overall system. This shows the message is send from source node. Source sends the message to intermediate nodes. Inside the buffer decision is taken. Finally the message reaches the destination.

Summary Vector Exchange Module:

The network information summarized as a summary vector is exchanged between the sender and the intermediate nodes, which includes the following data: Statistics of inter encounter time of every node pair maintained by the nodes Statistics regarding the buffered messages, including their IDs, remaining time to live (Ri), destinations for each incoming message.

Network State Estimation Module (NSEM):

The NSEM is used to obtain the estimated mi (Ti), ni (Ti), and si (Ti) Where, mi (Ti) – Number of nodes who have seen message i ni (Ti) - Number of copies of the message si (Ti) – Number of nodes who have seen message i and their buffers were not full.

Utility Calculation Module: UCM is used to optimize the average delivery ratio or delivery delay.
Decision: The decision of forwarding or dropping the buffered messages is made.

IV. Results and Analysis

Fig. 4.1-4.4 shows the experimental result of four modules. Fig 4.1 shows the Node formation. Fig 4.2 shows Analysis the trust node list. Fig 4.3 shows the SPN model.

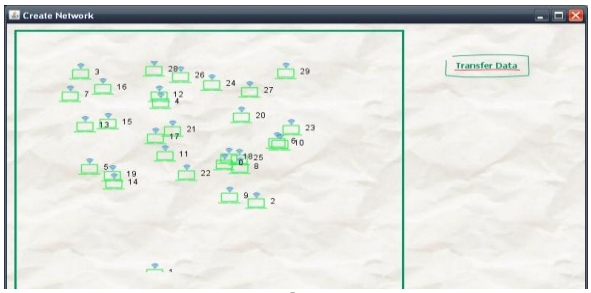
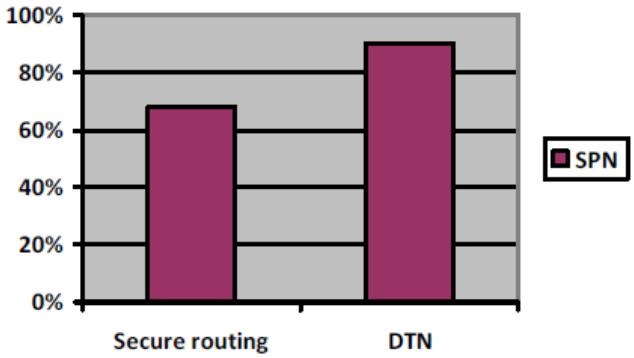


Fig.4.1Node Formation

Fig.4.2 Analysis the trust node list

Fig.4.3 SPN model



THE DECISION

Case	Entropy	Frequency	Conclusion	Score
1	High ($> \alpha$)	High ($> \beta$)	Potential	b_1
2	Low ($\leq \alpha$)	High ($> \beta$)	Medium threat	b_2
3	High ($> \alpha$)	Low ($\leq \beta$)	Potential later	b_3
4	Low ($\leq \alpha$)	Low ($\leq \beta$)	No threat	$b_4 = 0$

The performance graph shows the message delivery ratio comparison with routing protocols and DTN. With the Epidemic scheme, whenever two nodes encounter each other, they exchange all messages they do not have in common. Therefore, the message copies are spread like an "epidemic" throughout the network to every node using the maximum amount of resources. With controlled flooding, a limited number of copies of each message are generated and disseminated throughout the network hop forwarding or source. We performed a comparative analysis of trust-based secure routing running on top of our trust management protocol with Bayesian trust-based routing and non-trust-based routing protocols (PROPHET and epidemic) in DTNs. Our results backed by simulation validation demonstrate that our trust-based secure 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.

V. Conclusion and Future Scope

It is concluded that a hierarchical trust management framework for epidemic and two-hop forwarding routing in homogeneous DTNs, aiming to optimize either the message delivery ratio or message delivery delay. The proposed framework incorporates a suite of novel mechanisms for network state estimation and utility derivation, such that a node can obtain the priority for dropping each message in case of full buffer. The future scope is to develop another type of routing schemes. (a) Devising and validating a decentralized trust management scheme for autonomous WSNs without base stations;(b) Investigating the impact of the cluster size and the trust update interval to the protocol performance and lifetime of a given WSN. Thus message delivery can be made faster better than the existing system. The packet delivery ratio can be estimated by using the routing schemes. Instead of using priority based method selection of node priority can be done with another scheduling scheme. Thus more delay can be reduced by using new techniques.

REFERENCES

[1] S. Kosta, A. Mei, and J. Stefa, ―Small World in Motion (SWIM): Modeling Communities in Ad- Hoc Mobile Networking,‖ 7th IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, Boston, MA, USA, June 2010.

[2] A. Mei, and J. Stefa, ―Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals, ‖ IEEE International Conference on Distributed Computing Systems, Genoa, Italy, June 2010, pp. 488-297.

[3] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott, K.Fall, and H. Weiss, "Delay- Tolerant Networking Architecture," RFC4838, IETF, 2007.

[4] S. T. Cheng, C. M. Chen, and I. R. Chen, "Dynamic Quota-Based Admission Control with Sub-Rating in Multimedia Servers, ''Multimedia Systems, vol. 8, no. 2, 2000, pp. 83 91.

[5] S. T. Cheng, C. M. Chen, and I. R. Chen, "Performance Evaluation of an Admission Control Algorithm: Dynamic Threshold with Negotiation," Performance Evaluation, vol. 52, no. 1, 2003, pp. 1-13.

[6] A. Jøsang, and R. Ismail, "The Beta Reputation System," Bled Electronic Commerce Conference, Bled, Slovenia, June 17-19 2002, pp. 1-14.

[7] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 7, no. 3, 2003, pp. 19-20.

[8] L. McNamara, C. Mascolo, and L. Capra, "Media Sharing based on Colocation Prediction in Urban Transport," 14th Annual International Conference on Mobile Computing and Networking, San Francisco, CA, USA, 2008.

[9] J. D. Musa, "Operational Profiles in Software- Reliability Engineering," IEEE Software, vol. 10, no. 2, March 1993, pp. 14-32.