Secure Dynamic Routing For Delay Tolerant Network Using Qos And Social Trust

M.Kalidass[1], P.Senthilraja[2]
Department of Computer Science and Engineering
[1, 2] Assistant Professor,R.V.S. Educational trust's group of institutions, Dindigul, India.

Abstract-*Delay tolerant networks are characterized by high end-to-end latency, frequent disconnection, and opportunistic communication over unreliable wireless links. The design and validate a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish and malicious nodes. A novel model-based methodology based on Stochastic Petri Net techniques for the analysis of my trust protocol and validate it via extensive simulation. A comparative analysis of my proposed routing protocol against existing trust-based and non-trust based protocols. The trust-based routing protocol can effectively trade off message overhead and message delay for a significant gain in delivery ratio. Approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead. The result deals with malicious nodes and trust related attack in DTN.*

Keywords-Delay tolerant networks, dynamic trust management, stochastic Petri Net

I. INTRODUCTION

Delay Tolerant Networks are relatively new class of networks wherein sparseness and delay are particularly high. In conventional Mobile Ad-hoc Networks [15], the existence of end-to-end paths via contemporaneous links is assumed in spite of node mobility. DTNs are characterized by intermittent contacts between nodes. DTNs links on an end-to-end path do not exist contemporaneously, and hence, intermediate nodes may need to store, carry, and wait for opportunities to transfer data packets towards their destinations. Therefore, DTNs are characterized by large end-to-end latency, opportunistic communication over intermittent links, error-prone links, and the lack of end-to-end path from a source to its destination. it can be argued that MANETs [11] are a special class of DTNs. Wireless Delay Tolerant Network is a new Networks class which is characterized by a long message delay and lack of a fully connected path between the source and the target nodes. As a result, the use of mobile nodes acting as a buffer between the one to other end and behave as a store and forward approach. The message moves to a new node when it appears in the range, similarly the messages reach their destinations. The message sending is an opportunistic procedure because the messages are sent in an opportunistic way. Because of its characteristics wide range of useful applications have been developed for DTNs and enable a new class of networking applications in the wireless network interface which increases popularity of mobile devices. DTNs relay carriers sharing which is the essential requirement, but this cannot be guarantee because selfish nodes can avoid participating for other messages. On other hand malicious node creates the black hole which carries out attacks by deliberately dropping messages. Overcome these attacks is a real challenge due to the connectivity and distributed nature of DTNs. DTN are resource constrained in nature to save its own resources and nodes may develop selfish behaviours. In which its drop the packet of other nodes to maximize its own credit or benefits. Such nodes increase the message drop probability and reduce the message delivery rate. A dynamic trust based approach to protect network from black hole and selfish attacks.

II. METHODOLOGY

Stochastic Petri Net

The analysis methodology is model-based and hinges on the use of a Stochastic Petri Net [20] mathematical model to probabilistically estimate node status over time, given an anticipated operational profile as input. The SPN outputs provide ground truth node status and can serve as the basis for "objective" trust evaluation. To compare "subjective" trust obtained through protocol execution with "objective" trust obtained through the SPN outputs to provide a sound theoretical basis for validating the algorithm design for dynamic trust management. The underlying semi-Markov chain[21] has a state representation comprising "places" in the SPN model. A node's status is indicated by a 5-component state representation (Location, Member, Energy, CN, UNCOOP) with "Location" (an integer) indicating the current region the node resides, "Member" (a boolean variable) indicating if the node is a member, "Energy" (an integer) indicating the current energy level, "CN" (a boolean variable) indicating if the node is compromised, and "UNCOOP" (a boolean variable) indicating if the node is cooperative.

Trust composition

Taking into consideration that communication devices in future mobile networks may be carried mostly by human operators, our trust protocol design incorporates both social trust properties deriving from social network in addition to the conventional QoS trust properties deriving from communication networks. Social trust includes honesty, intimacy, selfishness, between ness centrality, and social reputation. A mobile network would consist of heterogeneous mobile devices carried by soldiers, robotic vehicles, or ground vehicles operated by humans. Therefore, unlike traditional network research, social trust must be considered between these mobile agents. Social networks to evaluate the social trust value of a node in terms of the degree of personal or social trends, rather than the capability of executing a mission based on past collaborative interactions. The latter belongs to QoS trust by which a node is judged if it is capable of completing an assigned mission as evaluated by communication networks.More specifically, QoS trust represents competence, dependability, reliability, successful experiences, and reputation or positive recommendations on task performance forwarded from direct or indirect interactions with others. The term QoS trust [10] to refer to trust evaluation in terms of task performance capability. To design dynamic trust management to allow a variety of social and QoS trust metrics to be explored and tested for their effectiveness.

Trust aggregation

Both direct observations and indirect recommendations to update trust. Separation of concerns for each social trust or Qos trust property selected. trust aggregation protocol for aggregating trust information of a trustee may use a distinct set of parameter settings for each trust property taking into account intrinsic properties of each trust property, so the “subjective” trust evaluation of the trustee node for that trust property is accurate.

Trust formation

Investigate and identify the best way to form the overall trust out of the selected social trust [10] and Qos trust properties in order to maximize application performance. Further, investigate a new design concept of application level trust optimization allowing an application to optimize the use of trust to classify nodes also for maximizing application performance.

Trust management

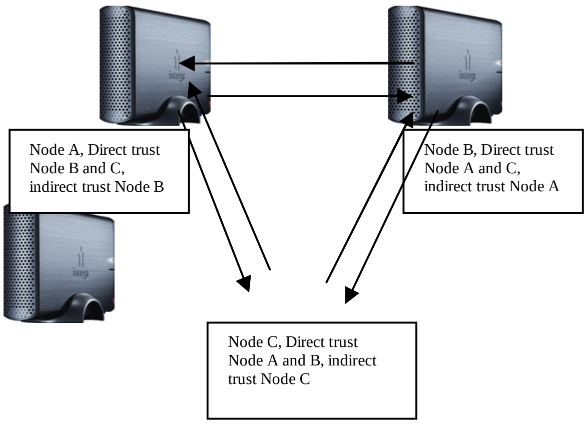
Network environment changes dynamically using trust value of each node. Without loss of generality, we consider environment changes in terms of increasing selfish and malicious nodes over time as modeled by the dashed line entities in the SPN model dynamically changing network conditions to minimize trust bias and to maximize DTN routing performance. Specifically, at runtime, each node senses hostility changes using its trust evaluation results.

Application-level trust optimization

The design concept of application-level trust optimization allowing an application to optimize the use of trust to classify nodes to maximize application performance. There are three applications built on top of dynamic trust management to demonstrate the validity of the design. (1) For the misbehaving node detection application, an optimal application-level drop-dead trust threshold, which a node is considered as misbehaving. By means of runtime trust evaluation, the dynamic trust management is made adaptive by adjusting the drop-dead trust threshold in response to changing environment conditions to minimize the false positive and false negative probabilities. (2) For the survivability management application, The best minimum trust level required for successful mission completion and the drop dead trust level to maximize the system reliability of mission execution with dynamic team membership. (3) For the secure routing application, the dynamically control a forwarding node trust threshold (FTT) and a recommender trust threshold (RTT) to classify nodes to optimize application requirements such as message delivery ratio and message delay.

III. SYSTEM ARCHITECTURE

Delay tolerant network 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 delay tolerant network routing. 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. 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 collocation information in urban transport environments for media sharing. Work is different from in that rather than by frequent collocation 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 lists. 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.


Node A, Direct trust Node B and C, indirect trust Node B
Node B, Direct trust Node A and C, indirect trust Node A
Node C, Direct trust Node A and B, indirect trust Node C

IV. EXPRIMENTAL RESULTS AND ANALYSIS

The numerical results generated from the SPN model. The trust evaluation results have two parts. The first part is about the convergence and accuracy of trust aggregation for individual trust properties. The second part is about maximizing application performance through trust formation and application-level trust optimization. Identifying the best way to form the overall trust out of QoS and social trust properties and the best way to set application-level trust parameters such that the application performance (i.e., secure routing) is maximized.

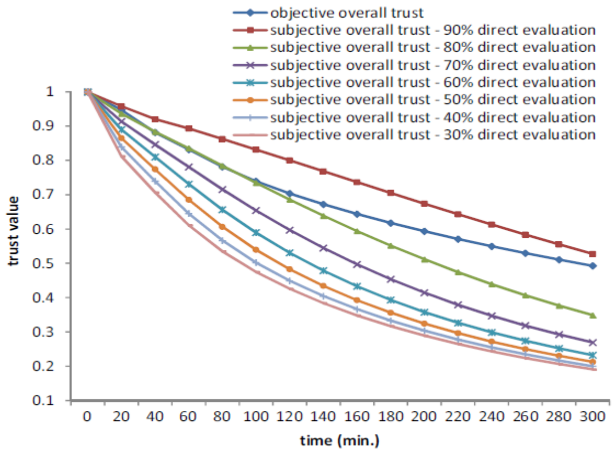
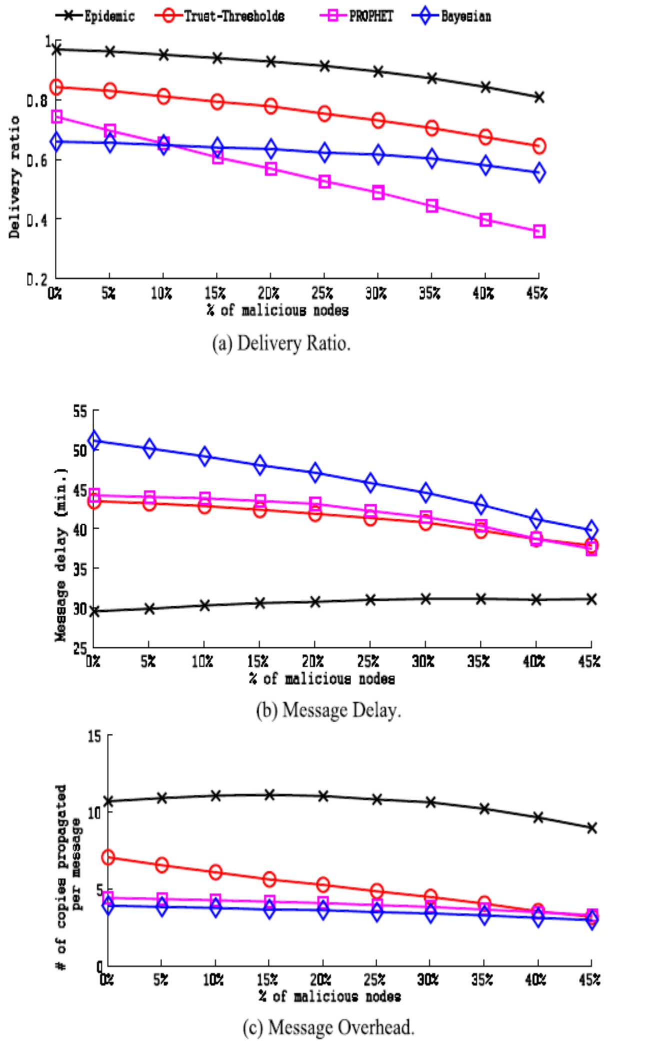


Figure 1:Overall Trust Evaluation

The node's overall trust values obtained from subjective trust evaluation vs. objective trust evaluation, also as a function of time. The subjective trust evaluation curve is reasonably close to the objective trust evaluation curve, but again there is a cutoff point after which the trust value is overestimated compared to objective trust. Initially, subjective trust evaluation undershoots due to lack of observations. At the later stage, nodes might be compromised and consume much resources. Therefore, subjective trust evaluation could overshoot compared to objective trust.



(a) Delivery Ratio.

(b) Message Delay.

(c) Message Overhead.

Figure 2:Performance comparison

The message delivery ratio, delay, and overhead generated by trust protocol against Bayesian trust-based, PROPHET, and epidemic routing protocols. The results demonstrate 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, 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. 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, trust-based routing protocol also outperforms Bayesian trust-based and PROPHET in message delay except when there is a very high percent of malicious nodes (e.g., 40- 45 percent of malicious nodes) in the system. The reason is that when there is a high percent of malicious nodes, protocol tends to use a higher weight for healthiness and consequently a lower weight for connectivity, thus causing a higher message delay. Here note that there is a tradeoff between message delivery ratio and message delay. When the percentage of malicious nodes in the network increases, a message originally successfully delivered with a longer message delay is more likely to be dropped; hence, this dropped message would not be counted in calculating message delay. This certainly does not mean should have more malicious nodes in the network since the message delivery ratio will decrease. The similar observations appear in investigating the performance of both message delivery ratio and message delay in DTN routing. Lastly, the message overhead of our trust-based routing protocol is significantly lower than epidemic routing. Trust-based protocol approaches the ideal performance of epidemic routing in delivery ratio and message delay without incurring high message overhead.

V. CONCLUTION AND FUTURE ENCHANCEMENT

The design and validate a trust management protocol for DTNs and applied it to secure routing to demonstrate its utility. Trust management protocol combines QoS trust with social trust to obtain a composite trust metric. Given an operational profile describing the network environment and node behaviors as input, 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 formation and application level trust setting, to be identified to maximize application performance. A comparative analysis of trust based secure routing running on top of our trust management protocol with existing trust-based and non-trust based routing protocols in DTNs. Plan to explore other trust-based DTN applications with which we could further demonstrate the utility of our dynamic trust management protocol design. plan to implement our proposed dynamic trust management protocol on top of a real DTN architecture to further validate the protocol design, as well as to quantify the protocol overhead. In future work is plan to explore other trust-based DTN applications with which further demonstrate the utility of our dynamic trust management protocol design. Also plan to implement proposed dynamic trust management protocol on top of a real DTN architecture to further validate the protocol design, as well as to quantify the protocol overhead.

REFERENCES

[1] “The ns-3 Network Simulator,” http://www.nsnam.org/, Nov. 2011.

[2] E. Ayday, H. Lee, and F. Fekri, “Trust Management and Adversary Detection for Delay Tolerant Networks,” Proc. Military Comm. Conf., pp. 1788-1793, 2010.

[3] E. Ayday, H. Lee, and F. Fekri, “An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks,” IEEE Trans. Mobile Computing, vol. 11, no. 9, pp. 1514-1531, Sept. 2012.

[4] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine, “Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking,”Proc. IEEE INFOCOM, pp. 1-11, Apr. 2006.

[5] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson, R. Durst, K. Scott,K. Fall, and H. Weiss, “Delay-Tolerant Networking Architecture,”RFC 4838, IETF, 2007.

[6] I.R. Chen, F. Bao, M. Chang, and J.H. Cho, “Supplemental Material for ‘Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing’,” IEEE Trans. Parallel and Distributed Systems, 2013.

[7] I.R. Chen and T.H. Hsi, “Performance Analysis of Admission Control Algorithms Based on Reward Optimization for Real-Time Multimedia Servers,” Performance Evaluation, vol. 33, no. 2, pp. 89-112, 1998.

[8] 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, pp. 83-91, 2000.

[9] 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, pp. 1-13, 2003.

[10] J.H. Cho, A. Swami, and I.R. Chen, “A Survey on Trust Management for Mobile Ad Hoc Networks,” IEEE Comm. Surveys & Tutorials, vol. 13, no. 4, pp. 562-583, Fourth Quarter 2011.

[11] E.M. Daly and M. Haahr, “Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs,” IEEE Trans. Mobile Computing, vol. 8, no. 5, pp. 606-621, May 2009.

[12] M.K. Denko, T. Sun, and I. Woungang, “Trust Management in Ubiquitous Computing: A Bayesian Approach,” Computer Comm., vol. 34, no. 3, pp. 398-406, 2011.

[13] V. Jacobson, D.K. Smetters, J.D. Thornton, M. Plass, N. Briggs, and R. Braynard, “Networking Named Content,” Comm. ACM, vol. 55, no. 1, pp. 117-124, 2012.

[14] A. Jøsang and R. Ismail, “The Beta Reputation System,” Proc. Bled Electronic Commerce Conf., pp. 1-14, June 2002.

[15] S. Kosta, A. Mei, and J. Stefa, “Small World in Motion (SWIM): Modeling Communities in Ad-Hoc Mobile Networking,” Proc. Seventh IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. And Networks, June 2010.

[16] F. Li, J. Wu, and A. Srinivasan, “Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets,” Proc. IEEE INFOCOM, pp. 2428-2436, 2009.

[17] N. Li and S.K. Das, “RADON: Reputation-Assisted Data Forwarding in Opportunistic Networks,” Proc. Second ACM Int’l Workshop Mobile Opportunistic Networking, pp. 8-14, Nov. 2010.

[18] Q. Li, S. Zhu, and G. Cao, “Routing in Socially Selfish Delay Tolerant Networks,” Proc. IEEE INFOCOM, pp. 1-9, Mar. 2010.

[19] A. Lindgren, A. Doria, and O. Schelen, “Probabilistic Routing in Intermittently Connected Networks,” ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 7, no. 3, pp. 19-20, 2003.

[20] K.S. Trivedi, “Stochastic Petri Nets Package User’s Manual,” Dept. of Electrical and Computer Eng. Duke Univ., 1999

[21] R. A. Sahner, K. Trivedi, and A. Puliafito, Performance and Reliability Analysis of Computer Systems: Kluwer Academic Publishers, 1996.