International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.12, December 2014 DOI:10.15693/ijaist/2014.v3i12.51-54

A Survey Of Trust Based Automatic Routing In Delay Tolerant Networks

Dr.M.BalaGanesh Associate Professor /Department of CSE,Anna University, Chennai,India

N.Nalini, PG Scholor /Department of CSE, Anna University, Chennai, India

***Abstract:*-Delay Tolerant Networks (DTNs) is the heterogeneous network which is used in the field of wireless communications.DTN are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. It consists of frequent disconnection and communication over an unreliable wireless links. The methods used for the protocol to validate extensive simulation and also the design and validation of dynamic trust management protocol for delay tolerant networks. The application used to gain the profit from Qos. It is based on trust based protocols and non trust based protocols. The comparison of both protocols the non trust based provides high incurring message of trusted nodes with message delivery ratio. The parameter occurred as unselfishness, perfect, energy and connectivity. The result deals with malicious nodes and trust related attack in DTN.**

Index Terms—Delay tolerant networks, quality of service, simulations and trust based protocols in DTN networks

I. INTRODUCTION

A delay tolerant network (DTN) comprises mobile nodes (e.g., humans in a social DTN) experiencing sparse connection, opportunistic communication, and frequently changing network topology. In DTN environment popular ad hoc routing protocols fail to establish routes. Fig 1.1 shows the lack of end to end connectivity in delay tolerant networks.

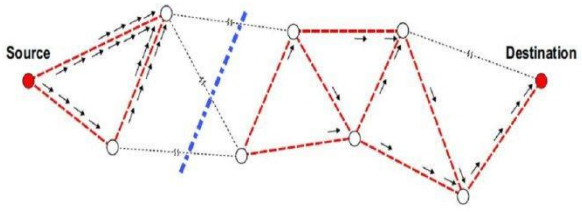

Fig 1.1 Lack of end to end connectivity in Delay tolerant Network

Because of lack of end-to-end connectivity, routing in DTN establish a store-carry-and-forward scheme, where data is incrementally moved and stored throughout the network in hopes that it will eventually reach its destination. Fig 1.2 shows the store-carry-and-forward scheme in Delay tolerant networks. Hence resulting in high end-to-end latency.

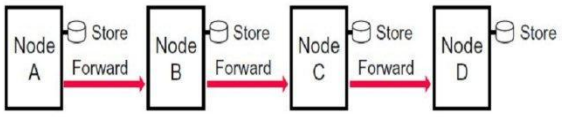

Fig 1.2 store-carry-and-forward scheme in DTN

A dispute is Trust management protocol design in DTN network is very exhibit a wide range of heterogeneous Qos characteristics are energy level, bandwidth, moving speed etc. It's based on performance and security requirements in a DTN are socially selfish to outsiders and unselfish to friends. The operation built on the DTN is trust based routing protocol[2] and to validate a dynamic trust management to optimize the population of maliciousnodes.

II. RELATED WORK

By the use of direct and indirect method in dynamic trust management to perform design analysis to secure routing . To adjust the trust parameter in threshold condition with respect to changing network dynamically.The efficacy of trust management protocol contains misbehaving node detection, selfish node detection, trust based survivability management in dynamic trust management protocol design. Delivery ratio is most important performance metrics for secure routing in mobile networks.Presence of well behaved selfish and malicious node in delay tolerant network validate the dynamic trust parameter and maximize the routing performance.

Consider a DTN environment with no centralized trusted authority. Nodes be in touch through numerous hops. When a node meets another node, they exchange encounter histories qualified by encounter tickets so as to avert black hole attacks to DTN routing. Idistinguish socially selfish nodes from

malicious nodes. A selfish node acts for its individual interests mutually with interests to its friends, groups, or communities. So it may drop packets randomly 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.

The combination of social trust deriving from social networks and quality of service it provide communication network into composite trust metric node in a DTN[10]. I consider the healthiness and unselfishness of two social metrics, the notation of subjective trust Vs objective trust based on ground truth of protocol. The combination of social trust from social networks and the traditional quality has a composite trust metrics to assess the trust nodes. Trust management and malicious node detection provides high data availability and packet delivery ratio with low latency in the presence of hackers.

Delay Tolerant Network communicates through energy, the comparison of Bayesian and PROPHET routing protocol[8] which can act as epidemic routing protocol. It is another form of dynamically changing environment in mobile network variables with each density nodes, such as number of misbehaving nodes.

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 (by providing bad recommendations against good 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).

A malicious attacker can perform random attacks to evade detection. Iintroduce a random attack probability P_{rand} to reflect random attack behavior. When P_{rand} =1, the malicious attacker is a reckless attacker; when P_{rand}< 1 it is a random attacker.

A collaborative attack means that the malicious nodes in the system boost their allies and focus on particular victims in the system to victimize. 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[1]. Imitigate 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 $T_f$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 evaluation and indirect trust information like recommendations. The trust of one node toward another node is updated upon encounter events. Each node will execute the trust protocol independently and will perform its direct trust assessment toward an encountered node based on specific detection mechanisms designed for assessing a trust property.

III SYSTEM MODEL

Our trust protocol considers trust composition, trust aggregation, trust formation and application-level trust optimization designs. Fig. 2 shows a flowchart of our trust management protocol execution.

I consider two types of trust properties:

QOS trust: QOS trust is evaluated through the communication network by the capability of a node to deliver messages to the destination node. Iconsider "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 function.

Social trust: Social trust is based on honesty or integrity in social relationships and friendship in social ties. I 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 friend-ship, I 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. I consider "healthiness", "unselfishness", and "energy" in order to achieve high message delivery ratio, and I consider "connectivity" to achieve low message delay.

The selection of trust properties is application driven. In DTN routing, message delivery ratio and message delay are two important factors. I consider "healthiness", "unselfishness", and "energy" in order to achieve high message delivery ratio, and

Iconsider "connectivity" to achieve low message delay.

In this trust model, a node's trust value is assessed based on direct trust evaluation and indirect trust information like recommendations. The trust of one node toward another node is updated upon encounter events. Each node will execute the trust protocol independently and will perform its direct trust assessment toward an encountered node based on specific detection mechanisms. A misbehaving node, which node may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good ties with the source, current carrier or destination node. Fig 5.1 shows delivery ratio under trust formation.

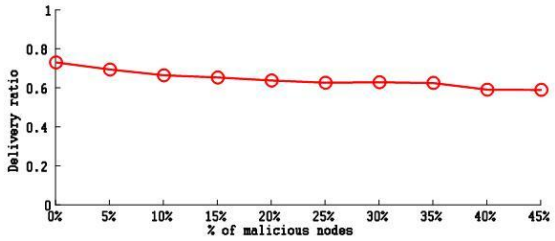

Fig 5.2 Delivery ratio under best trust formation

IVCONCLUSION

In this paper, Idesigned and validated a trust management protocol for DTNs and applied it to secure routing to demonstrate its utility. Our trust management protocol combines QoS trust with social trust to obtain a composite trust metric. Our 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. Further, our design also allows the best trust formation and application-level trust settings be identified to maximize application performance. I demonstrated how the results obtained at design time can facilitate dynamic trust management for DTN routing in response to dynamically changing conditions at runtime.

REFERENCES

[1] Ing-Ray Chen, Member, IEEE, FenyeBao, MoonJeong Chang, and Jin-Hee Cho, Member, IEEE

[2] "The ns-3 Network Simulator," http://www.nsnam.org/, Nov. 2011.

[3] E Ayday, H. Lee, and F. Fekri, "Trust Management and Adver-sary Detection for Delay Tolerant Networks," Proc. Military Comm. Conf., pp. 1788-1793, 2010.

[4] 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.

[5] 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.

[6]V.Cerf,S.Burleigh,A.Hooke,L.Torgerson,R.Durst, K.Scott, K. Fall, and H. Weiss, "Delay-Tolerant Networking Architec-ture,"RFC 4838, IETF, 2007.

[7] 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.

[8] 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.

[9] S.T. Cheng, C.M. Chen, and I.R. Chen, "Dynamic Quota-Based Admission Control with Sub-Rating in Multimedia Servers," Mul-timedia Systems, vol. 8, no. 2, pp. 83-91, 2000.

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

[11] J.H. Cho, A. Swami, and I.R. Chen, "A Survey on Trust Manage-ment for Mobile Ad Hoc Networks," IEEE Comm. Surveys &Tuto-rials, vol. 13, no. 4, pp. 562-583, Fourth Quarter 2011.

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

Authors Profile

N.Nalinireceived the **B.E.** degree in computer science engineering from the J.J College of Engineering, Trichy, Anna University, Chennai, India, in 2007.Currently doing **M.E.** in computer science engineering in sembodairukmanivarathar ajan college of engineering and technology, vedaranyam,Tamilnadu India. Her research interest includes communicationnetworks, Mobile Ad hoc networks, Delay tolerant Networks.