# Delay Tolerant Networks on Trust Based Dynamic Data for Secure Routing

**Suganya.S** [1]

**MAM College Of Engineering**

**Trichy,Tamilnadu**

**suganyabtech67@gmail.com**

**M. Anandha Kumar**[2]

**MAM College Of Engineering**

**Trichy,Tamilnadu**

**anandhme005@gmail.com**

***ABSTRACT*:The delay tolerant networks (DTNs) are high end-to-end latency and numerous disconnection and characterized opportunistic communication over unreliable wireless links. In DTN environment the Dynamic trust management protocol is designed and validate for secure routing optimization in the being there of well-behaved, selfish and malicious nodes. The system develops a methodology for the analysis of the trust protocol and validates it through extensive simulation. Furthermore, the address dynamic trust management that is to determine and apply the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance. A proportional study of the proposed routing protocol against Bayesian trust-based and non-trust based (PROPHET and epidemic) routing protocols. The results make obvious that the protocol is able to deal with selfish behaviors and is resilient against trust-related attacks. In addition, the trust based routing protocol can effectively trade off message above your head and message delay for a significant gain in delivery ratio.**

**Key Terms—Delay tolerant networks, dynamic trust management, secure routing**

## 1 INTRODUCTION

The dynamic trust management for DTNs to deal with both malicious and selfish misbehaving nodes. The notion of selfishness has been social selfishness[5] as very often humans carrying communication devices in smart phones in a DTN are socially selfish to outsiders but unselfish to friends. The notion of maliciousness refers to malicious nodes performing trust-related attacks to disrupt DTN operations built on trust. 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 through secure Router.

Social network obtained from the social trust and communication network obtained from the traditional quality of service into a composite trust metric to assess the trust of a node in a DTN. The validation of the protocol is based on the notions of subjective trust versus objective trust. In response to changing conditions to maximize DTN routing performance dynamically for protocol and adjust to the trust aggregation and the

system address the issue of application performance maximization. The analysis of the trust protocol and validation is done on the stochastic petri net (SPN) techniques[9]. The dynamic trust management validates the protocol against routing based on Bayesian trust management protocol. Further, it approaches the performance of epidemic routing in delivery ratio and message delay without incurring high message or protocol maintenance overhead.

## 2 RELATED WORK

[1] Delay Tolerant Networks (DTNs) are relatively new class of networks, where in sparseness and delay are particularly high. In conventional Mobile Ad-hoc Networks (MANETs), the existence of end-to-end paths via contemporaneous links is assumed in spite of node mobility[10]. In contrast, DTNs are characterized by intermittent contacts between nodes. In other words, DTNs' links on an end-to-end path do not exist contemporaneously, and hence, intermediate nodes may need for storing, carrying, and waiting for opportunities to transfer data packets towards their destinations.

Despite all the progress for securing MANETs, achieving the same for DTNs leads to additional challenges. The special constraints posed by DTNs make existing security protocols impractical in such networks. Common techniques[10] to build reputation in MANETs are based on the direct measurements of a suspicious node, acknowledgement (ACK) messages from the destination, and indirect measurements of the suspicious nodes.. The proposed algorithm computes the reputations of the network nodes accurately in a short amount of time in the presence of attackers without any central authority. The proposed algorithm has a computational complexity that is linear with the number of nodes in the network. Hence, it is scalable and suitable for large scale implementations.

[2] Delivering multimedia streams with QoS requirements to viewers is one crucial issue in designing a multimedia system. Upon the arrival of a new request, the server decides if the request can be admitted based on the availability of the server capacity. QoS guarantee of continuous multimedia stream delivery is met once it is admitted. One mechanism for admission control is based on the reservation scheme. The reservation scheme allocates a fraction of the server capacity (e.g. CPU time and network bandwidth) for a new request based on certain criteria. A new request may be rejected if no available resource is left to serve the request. In such a case, the system incurs a loss due to the rejected requests.

On the one extreme, the algorithm used for controlling the admission is the deterministic approach, and at another is the observation based approach. The latter approach is based on the prediction from the measurements of the resource usage status and provides a predictive service guarantee to clients, not an absolute guarantee. The propose system shows the dynamic quota-based algorithm with sub-rating mechanism. The sub-rating method will reduce the QoS of several low-priority clients by cutting out a small fraction of the assigned server capability, to accept a new high-priority client and to achieve a higher net earning value.

[3] Delivering multimedia streams with QoS requirements to viewers is one crucial issue in designing a multimedia system. Upon the arrival of a new request, the server decides if the request can be admitted based on the availability of the server capacity. One mechanism for admission control is based on the reservation scheme. The reservation scheme allocates a fraction of the server capacity for a new request based on certain criteria. . A new request may be rejected if no available resource is left to serve the request. The deterministic approach derives a formula of the maximum number of admitted requests under the worst-case load. The requests are

assured of their QoS requirements throughout their existence in the system.

The research does not consider different priorities of client requests. Most research tries to admit as many requests as possible without considering the importance of each request. The clients may offer high value of reward and should be given to services which has priority. Similarly, the system has to pay high penalty for a high-priority request when it rejects. The propose performance analysis models for the mechanism. The analytical models can be used to dynamically determine the optimal setting of threshold values in real-time upon the modifying the system load , in which the system workload is characterized by the arrival rate, service rate, reward rate, and penalty rate of each client.

[4] Hard security, such as providing cryptography protection can help maintain partial security by providing data confidentiality, data integrity, authentication and no repudiation within networks, and has achieved much coveted coverage as a research field in recent times. However, hard security can be vulnerable if somebody successfully finds a way to by-pass the security arrangements or the components do not operate as expected. For example, hard security cannot protect against nodes that may act legitimately initially, but then become compromised or act selfishly after the hard security event. There is a requirement to defend against the threat of behavioral changes. This is known as soft security.

It means that future research should include investigations into incorporating node heterogeneity into trust algorithms, but with different functional descriptions to consider calculating trust between heterogeneous nodes also creates a challenge as to how to determine the normal behavior of an unknown node without increasing the complexity of trust computations. Nodes could also be of high mobility mounted on a fast moving vehicle. This means that the network composition changing in an unpredictable manner. The highly dynamic nature of mobile ad-hoc networks ensures the difficulty to associate information and node behavior with node locations. Existing research currently has not provided a detailed analysis or addressed the challenge of determining a potential measurable relationship between node mobility, network density and link dynamics with trust propagation.

[5] Delay Tolerant Networks (DTNs) enable data transfer when mobile nodes are only intermittently connected. Due to lack of consistent connectivity, DTN routing used to follow store-carry-and-forward. After receiving packets, a node carries them around until it contacts another node and then forwards the packets. Since DTN routing relies on mobile nodes to forward packets for each other, the routing performance (e.g., The number of packets, delivered to their destination) depends on if nodes are willing to forward to others. In the real world, most people are socially selfish. As has been social, they are willing to forward packets for others with whom they have social ties such as family members and friends even at the cost of their own resources.

As far as we know, social selfishness have not been addressed before. Although many routing algorithms have been proposed for DTNs, most of them do not consider user willingness and implicitly assume that a node is willing to forward packets for all others. Since each node only forwards packets to part of the nodes, it is important to notice that how it will affect the performance of routing. To achieve high performance, SSAR considers both user willingness and contact opportunity when to select relays. It combines the two factors through mathematical modeling and machine learning techniques, and obtains a new metric to measure the forwarding capability of a relay.

## 3 SYSTEM MODEL

In DTN routing a black hole attack is prevented by exchange encounter histories certified by encounter tickets when a node encounters another node. A DTN environment with no centralized trusted authority [5]. Through multiple hops a node can communicate. A selfish node acts in its own interests, including the interests of its groups, or communities. So it may drop packets by chance to save energy, but it can decide to forward a packet if it has good social ties with the source, current carrier or destination node. It considers a friendship matrix to represent the social ties among nodes. The modules are Channel available checking module, Dynamic trust management process module, Secure Routing enabled module, Adjust and Update Trust Level.

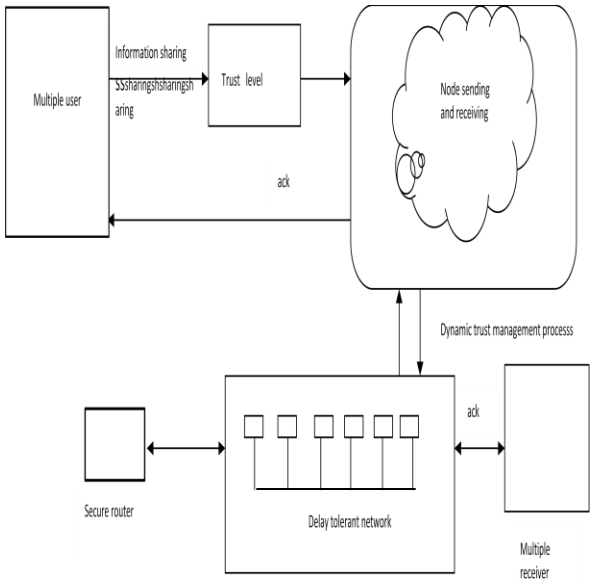


Fig 1system architecture

**Channel available checking module:** Across all maximum achievable throughputs is either given based on measurements under perfect conditions or in channel data rates [3]. On the other hand does not reach the area or particular system in which data is being transferred between two endpoints of which at least one is typically connected to a wired infrastructure or wireless networks and the other endpoint is connected to an infrastructure via a wireless link.

**Dynamic trust management process module:** Dynamic trust management protocol DTN routing against PROPHET [5], Bayesian trust-based routing, and epidemic routing, all operating under best protocol settings dynamically in response to hostility changes over time. Data's are continuously sent to the source to destination, but the dynamic trust management algorithm is changed Non-trusted protocol to Trusted protocol is well. Sender Nodes communicate through multiple hops from wireless communication source to destination. Differentiate socially selfish nodes from malicious nodes. A selfish node acts in its own interests, including the interests of its friends, groups, or communities change without owner's permission.

**Secure Routing module:** The network connections are dropped that time enables 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 [4]. In addition to packets dropping, 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. The basically the consequence of integration of trust and security metrics into routing and replication decisions in DTNs construct Secure Packet Bundled Temporarily.

**Adjust and Update Trust Level:** In DTN routing, message delivery ratio and message delay are two important factors. It considers "healthiness", "unselfishness", and "energy" in order to achieve a high

message delivery ratio, and 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 latency, frequent disconnection, and opportunistic communication over untrustworthy wireless links so adjust and update the nodes dynamically. The trust protocol considers trust composition, trust aggregation, trust formation and application-level trust optimization designs. Social trust is based on honesty or integrity in social relationships and friendship in social ties.

## 4 TRUST MANAGEMENT PROTOCOL

The Trust composition design has two types of trust properties:

1. QoS trust is evaluated through the communication network with the capability of a node to deliver messages to the destination node. To measure the QoS trust level of node it considers as connectivity and energy. The connectivity QoS trust is about the ability of a node to encounter other nodes due to its movement patterns. The energy level is about the battery energy of a node to perform the basic routing function.

2. Social trust is based on honesty or integrity in social relationships and friendship in social ties. A node of social trust is measured by It considers as healthiness and social unselfishness. The healthiness social trust is the belief of whether a node is malicious. The unselfishness trust is the belief of whether a node is socially selfish. While social ties cover more than just friendship, it is considered friendship as a major factor for determining a node's socially selfish behavior.

$$T_{i,j}(t)=\sum_{x}^{all} w^x \times T_{i,j}(t) \qquad (1)$$

where x represents a trust property explored, $T_{i,j}(t)$ is node i is trust in trust property x in the neighborhood of node j, and $w^x$ is the weight associated with trust property X with the sum equal to 1. $w^x$ is application dependent. It is not related to the priority of the application, but dependent on the operational profile of an application. The best weight ratio under which the application performance is maximized, given an operational profile as input.

## 5 NUMERICAL RESULTS

The concept of operational profiles in software reliability engineering as we build the numerical model [8]. An operational profile is what the system expects to observe during its operational stage. During the testing and debugging phase, a system would be tested with its anticipated operational profile to reveal design error. Failures are detected and design faults causing system failures are removed to improve the system consistency.

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 ($E_0$) of each node represented by a number of tokens is assigned according to node heterogeneity information. A token is taken out when transition T_ENE[3] 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_ENE[3] indicates the energy consumption rate which varies depending on the ground truth status of the node. The operational profile specifies the energy consumption rate of a malicious node versus a selfish node versus a well-behaved node.

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

Unselfishness: A socially selfish node drops packets except the source, current carrier or the destination node is in its friend list. It will know the ground truth status of

unselfishness, of the node by simply inspect if place selfishness contain a token.

Dynamically changing environmental conditions: With the goal to deal with malicious and selfish nodes in DTN routing, a dynamically changing environment in which the number of bad nodes is changing over time. A node becomes malicious if it is captured and turned into a compromised node, as dictated by the per node capture rate.

Objective trust evaluation: The SPN model described above yields actual or ground truth status of each node. The "objective" trust of node j at time t, denoted by Tj (t), is also obtained from Eq.(1).

## 6 CONCLUSION

The designed and validated a trust management protocol for DTNs and applied it to secure routing to demonstrate its utility. The trust management protocol combines QoS trust with social trust to obtain a composite trust metric. The design also allows the best trust formation ($w^x$ )and application level trust settings (Tf; Trec) to be identified to maximize application performance. The system demonstrated how the results obtained at design time can facilitate dynamic trust management for DTN routing in response to changing conditions at runtime. The analysis of trust-based secure routing running on top of our trust management protocol with Bayesian trustbased routing and non-trust-based routing protocols.

## REFERENCES


1.E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," Proc. Military Comm. Conf., pp. 1788-1793, 2010.

2. 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.

3.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.

4.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.

5.A Survey of Trust Management in Mobile Ad-Hoc Networks Philip England, Dr Qi Shi, Dr Bob Askwith, Dr Faycal Bouhafs, School of Computing and Mathematical Sciences, Liverpool John Moores University, Liverpool, UK P.England@2011.ljmu.ac.uk, Q.Shi@ljmu.ac.uk, R.J.Askwith@ljmu.ac.uk, F.Bouhafs@ljmu.ac.uk

6.A routing protocol for socially selfish delay tolerant networks Qinghua Li, Wei Gao, Sencun Zhu, Guohong Cao Department of Computer Science & Engineering, The Pennsylvania State University, University Park, United States.

7. 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.

8. 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.

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

10. K.S. Trivedi, "Stochastic Petri Nets Package User's Manual," Dept. of Electrical and Computer Eng. Duke Univ., 1999.