International Journal of Engineering &Technology, 7 (3.12) (2018) 726 -728

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper



Energy Efficient Routing and Peer to Peer Trust Assessment for Increasing the Network Life Time in Delay Tolerant Networks

S. Murugaveni[1*], B.Priyalakshmi[2], K.Vijayan[3]

[1, 2, 3]Department of TCE
SRM University, Chennai
**Corresponding Author E-mail: veniharshini@gmail.com*

Abstract

In military network environments is resource-constrained arrange conditions, where end-to-end network is not ensured because of successive deferral, an efficient solution is required for trustful and energy efficient routing. Proposed work, provenance trust based routing is combined with energy efficient route to opt for a high network lifetime. Proposed scheme is designed for peer-to-peer trust assessment and maximize the delivery of correct messages received by destination nodes while minimizing message delay and communication cost Provenance alludes to the historical backdrop of responsibility for esteemed data. Proposed scheme avoids malicious node using provenance model and achieves good network lifetime using energy efficient routing strategy. Node's trust is calculated dynamically in response to changes in the environmental and node conditions.

Keywords: *Energy productivity, entrepreneurial steering, hand-off hub, remote sensor.*

1. Introduction

Delay tolerant systems (DTNs) are frequently discovers applications in different fields, for example, crisis reaction, extraordinary operations, shrewd conditions, earthly situations and vehicular impromptu systems, where several nodes participate in group communications to achieve a common mission. The core characteristic of DTNs has no assurance on end-to-end availability, along these lines causing a high deferral in the system. Information provenance has been utilized to examine the logical information in numerous applications. Data provenance is sometimes describing the origins of a piece of data and how the data achieves the current state. A major challenge of a provenance-based system is that it must protect against aggressors who may interfere with roll out improvements or drop messages including provenance data or spread the fake data. Quality of data source depends on the idea of provenance, this work propose a provenance based trust model, called PROVEST (PROVENANCE based Trust model), that aims to answer the challenge. Though provenance verification enhances the security of network, the work may lag in energy efficient routing. Thus it is energy of nodes will be considered along with provenance, which ensures the energy efficient and secure routing in delay tolerant network.

2. Related Work

There are a few investigations in light of steering related parameters, similar to availability parameters and thickness of the circulated hubs, in 1-D line networks.[1],[5]
examined Communication systems, regardless of whether they are wired or remote, have been thought to be associated. Nonetheless, rising applications, for example, crisis reaction, uncommon operations, keen situations and so on combined
with hub and unstable connections changes the regular conditions under which systems work. Truth be told, all things considered, systems might be generally separated. In this way more often than not, end-to-end ways associating each hub combine don't exist. To adapt up to visit, seemingly perpetual disengagements, astute directing procedures have been proposed in which, at each jump, a hub developing number of such checks whether it ought to forward or store-and-convey that message. Despite recommendations, there still exists little concession to the most appropriate directing algorithm(s) in this unique circumstance. One reason of rising remote applications and systems showing such "rambling" availability is the huge assorted qualities. Trust administration for experience based steering in postpone tolerant systems investigated by [2-4] ie. Propose and break down a class of trust administration conventions for experience based directing in postpone tolerant systems (DTNs)[3]. The thought is to join put stock in assessment in the steering convention, considering nature of-benefit (QoS) as well as trust properties and social trust properties additionally to assess different hubs experienced.

3. System Architecture

In our system we proposed a provenance based trust model for secure group communication in DTN environment. where communication occurs through a symmetric key which is known as unique key. During the message transfer node did not know whether the neighbor node deliver the packet to the destination node or not so we classify the node into three categories, POSITIVE, NEGATIVE, and UNCERTAIN.

POSITIVE NODE - When neighbor node deliver the packet to the destination node is known as positive node.

Copyright © 2018 Authors. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

UNCERTAIN NODE - when node can't check the neighbor node on encounter due to the short contact time is classified as uncertain.
NEGATIVE NODE - If neighbor node can't deliver the packet due to the presence of attacker and malicious node is known as negative node.

Network Model:

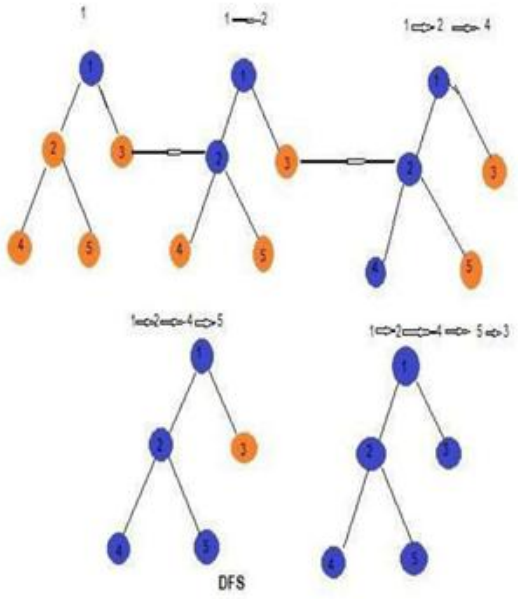
Hubs not just communicate with each other to convey the message additionally to trade the data. Source hub sends the data towards goal hubs in light of the past experiences. For message conveyance hubs utilize "store and forward" procedure, which implies hub stores the message until the point that it experiences a message bearer. Every hubs doesn't know the hubs area and their portability designs because of the idea of store and forward message conveyance, hubs are having heterogeneous qualities like vitality level observing abilities co-operations probabilities (parcel dropping), fake personalities and message change checking [8-10].

ENERGY LEVEL - Source node checks the threshold energy level of neighbor nodes and then deliver the message.

DETECTION ERROR - It checks if any node in between modifies the message and inform source node so that it can send the message through different path.

Depth First Search Algorithm:

This algorithm is used when an attacker or malicious node encounters in between the path of message delivery, it is a recursive algorithm that uses the idea of back tracking, the word back tracking means when the messages going on and suddenly encounters the malicious or attacker node then it goes back on the same path to find nodes to traverse [6-7].



Diffie-Hellmen Algorithm:

It is an algorithm used to establish a shared secret between two nodes. It is a method of securely exchanging cryptographic keys over the public channel. It is also called exponential key exchange. Asymmetric Encryption of data requires transfer of cryptographic self-contained key. The most challenging part in this type of encryption is the transfer of the encryption key from sender to receiver without any intercepting key in between. This transfer on same cryptographic keys at both sides secretively was made possible by the Diffie-Hellman algorithm. The basis of its calculation uses arithmetic modulus algorithm. Suppose Alice and Bob follow this key exchange procedure with Eve acting as a man in middle interceptor (or the bad guy).

Output Graph:

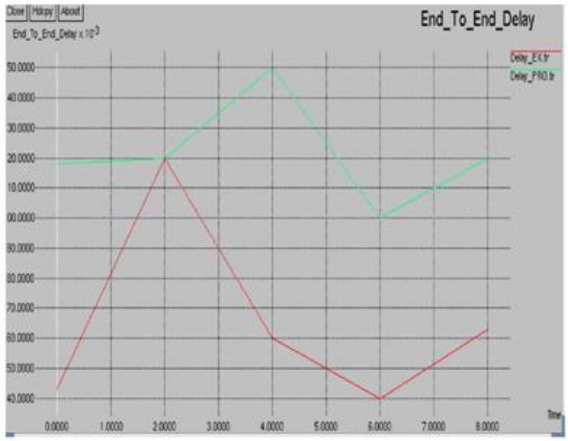


Fig. 1: Graph gives the comparison of delay between existing and provest model i.e. time between 2 packets

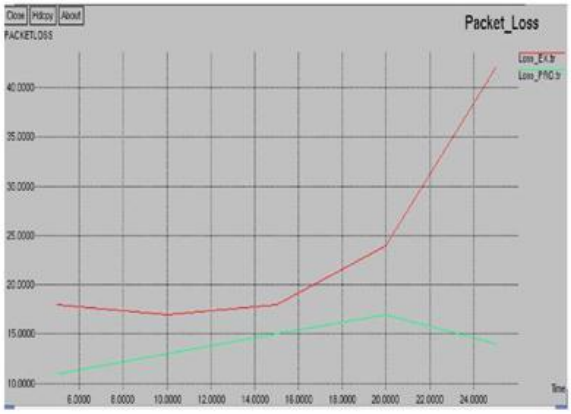


Fig. 2: Graph show the packet loss comparison between provest and existing model

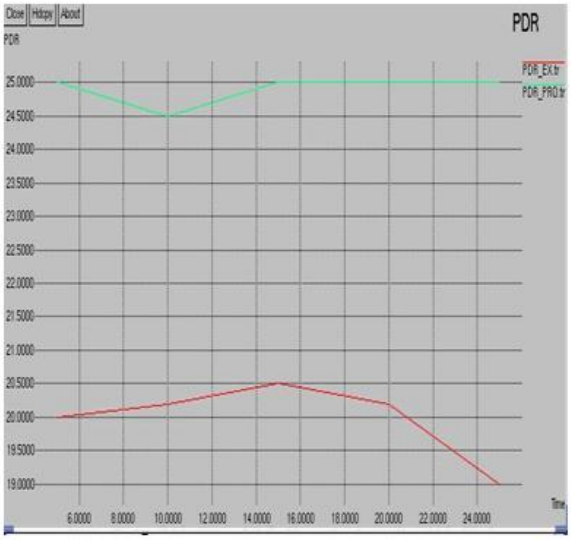


Fig. 3: Graph shows the packet delivery rate comparison between provest and existing model

4. Conclusion

A Provenance-based trust model called PROVEST which evaluates trust of a node by leveraging the provenance information added by each intermediate message carrier as indirect evidence during message forwarding. PROVEST performs adaptive control based on the historical pattern of evidence such as positive or

negative evidence. This feature excels in identifying bad nodes in the network where trust evidence is uncertain. Provenance-based approach significantly reduces the communication cost while maintaining a high correct message delivery ratio.

Reference

[1] T.Spyroulous, R.Rias, T.Turletti, K.Obracz ka,and A.Vasilakos, "Routing for disruption tolerant networks taxonomy and design", Wireless networks, vol.16, no.8, pp.2349-2370, 2010.

[2] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho,'Trust management for encounter – based routing in delay networks, in IEEE Global Telecommunications conference, Miami, FL, 6-10 Dec. 2010,pp. 1–6., Dec. 2010

[3] "Dynamic trust management for delay tolerant networks and its application to secure routing," IEEE Transactions on parallel distributed systems, vol 25, no 5, pp.1200-1210, May 2014.

[4] P. Buneman, S. Khanna, and W. Tan, "Why and where: A characterization of data provenance," in Proceedings of International Conference on Database Theory, Springer-Verlag, pp. 316–330, 2001.

[5] J.-H.Cho, M.Chang, I.-R.Chen, and A.Swami, "Trust Management VI IFIP", Advances in Information and Communication Technology.

[6] G. McDonald, L. O. Murchu, S. Doherty, and E. Chien, "Stuxnet 0.5: The missing link", Symantec Security Response [online], vol. 26, 2013.

[7] B. Bencsath, G.P´ ek, L. Butty´an, and M. F ´ elegyh´azi, "The cousins of ´ stuxnet: Duqu, flame, and gauss", Future Internet, vol. 4, no. 4, pp. 971–1003, 2012.

[8] J. Menn, "Key internet operator verisign hit by hackers," Reuters, feb, vol. 2, 2012

[9] Prosecutors and Public, "Messiah spyware infects middle east targets".

[10] M. Balduzzi, V. Ciangaglini, and R.McArdle, "Targeted attacks detection with spunge", Trend Micro Research, EMEA, 2013.