ISSN:0975-9646

A Review of Trust Model in Delay Tolerant Network

Ashwini Borkar
Department of Computer Science and Engineering
G.H Raisoni Institute of Engineering and Technology for Women
Nagpur, India

***Abstract*— Malicious and selfish behavior of node can cause serious threats in delay tolerant network. Thus designing a misbehavior scheme is a great challenge in DTN. We propose a trust model on the basis of packet drop level detection. The basic idea of trust model is introducing a periodically available trusted authority (TA). TA launches probabilistic detection for the target node and judge it by collecting the forwarding history. It reduces verification cost incurred by routing evidence phase. It also allows trusted authority to launch the misbehavior detection at a certain probability. It makes a proper communication between the sink node and the receiving node and transfer data over multiple router.**

***Keywords*—** *misbehavior detection, delay tolerant network, evidence phase.*

I. INTRODUCTION

Delay tolerant network is an approach to computer network architecture that seeks to address the technical issues in heterogeneous network. It may lack continuous network connectivity. Example of these networks are those operating in mobile, or planned networks in space, or extreme terrestrial environments.

In delay tolerant network, number of messages can be sent over to an existing link and store there until next link appears. Recently, the tern disruption tolerant network has gained currency in the United States due to support from DRAPA, which has funded many DTN projects. Disruption may cause because of the limits of wireless radio range, energy resources and noise or sparsity of mobile nodes.

A delay-tolerant network is a network designed to operate effectively over long distances such as those encountered in space communications or on an interplanetary scale. In such environment, long latency sometimes measured in hours or days, is inevitable. However, when interference is extreme or network resources are severely overburdened, similar problems can also occur over modest distances. DTN involves some of the same technologies as are used in a disruption tolerant network but there are important distinctions. A delay-tolerant network needs hardware that can store large amount of data. Such media must be able to survive extended power loss and then system restarts. It must be immediately accessible at any time. Ideal technologies for this purpose include high-volume flash memory and hard drives. The data stored on these media must be organized and prioritized by software which ensures accurate and reliable store-and-forward functionality.

In a delay-tolerant network, traffic can also be classified in three ways i.e. expedited, normal and bulk in order of their decreasing priority. Expedited packets are always transmitted, and verified before data of any other class from a given source to a given destination. Normal traffic is sent after all expedited packets have been successfully assembled at their fixed destination. Bulk traffic is not dealt with until all packets of other classes from the same source and bound for the same destination have been successfully transmitted and verified. The proposed trust scheme is inspired from inspection game, a game theory model in which inspector verifies if inspectee is violating the rules.

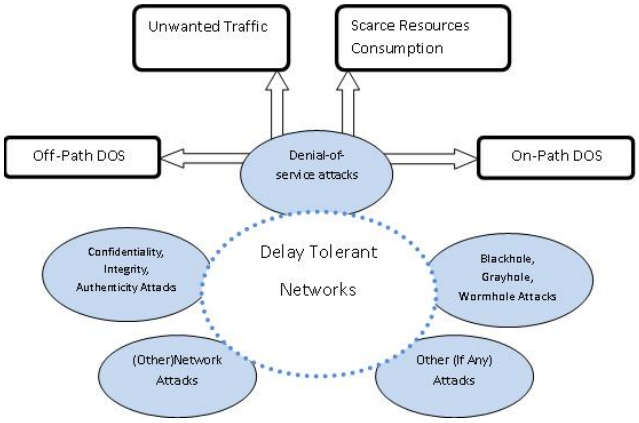

Fig.1. System Architecture

II. SYSTEM MODEL AND DESIGN GOALS

System model:
In system model, we consider a DTN network. DTN consisted of mobile devices owned by individual users. The nodes that are present in the network have their unique ID. We assume that the trusted authority exists so that it could take the responsibility of misbehavior detection in DTN. If there are number of nodes in the network, the trusted authority collects all the information and find out whether the node is trusted or not.

Design Requirements:

A. Distributed

We require a trusted authority that could take responsibility of misbehavior scheme.

B. Robust

We require misbehavior detection scheme that could tolerate various forwarding failure.

C. Scalability

We require a scheme that is independent of the size of the network.

III.THE PROPOSED BASIC SCHEME IN DTN

Trust: There are several definitions given to trust in the literature. Trust is always defined by reliability, utility, availability, quality of services and other concepts. Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to previous observation of behaviours i.e., the trust value is used to reflect whether a sensor node is willing and able to act normally in wireless sensor networks. There are three kinds of trust given as follows:

Direct Trust: Direct trust is a kind of trust which is calculated
on the basis of direct communication behaviours. It reflects the trust relationship between two neighbouring nodes.

Recommendation Trust: There is an efficient mechanism to filter the recommendation information. The filtered reliable recommendations are calculated as the recommendation trust.

Indirect Trust: When a subject node cannot directly observe an object nodes communication behaviours, indirect trust can be established. The indirect trust value is gained based on the recommendations from other nodes.

As shown in fig, the trust has two phases that are routing evidence generation phase and auditing phase. In the routing evidence generation phase, nodes will meet another node and send the forwarding history to different nodes. In the auditing phase, trusted authority will detect whether the node is trusted or not.
Suppose node A has packets which has to be delivered to node C. Now if node A meets another node B that could help to deliver packets to C, then node A will forward those packets to B. Thus, B could forward the packets to node C when C arrives at the transmission range of B.
There are three steps in the routing evidence generation phase that could be used to judge if a node is a malicious one or not.

a) Delegation task evidence
b) Forwarding history evidence
c) Contact history evidence

In the routing evidence phase, A sends packet to B, then it gets the delegation history back. B holds this packet, then faces C and C gets the contact history about B.

In the auditing phase, trusted authority will broadcast a message to ask all the other nodes to submit the evidences about B, when TA decides to check B. Then A submits the delegation history about B and C submits the contact history about B.

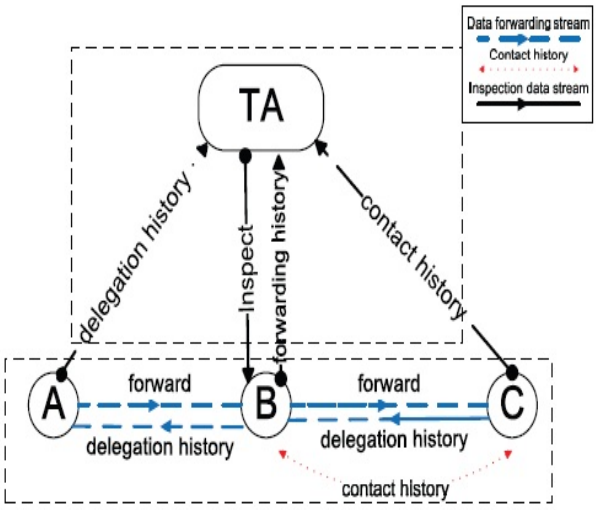

Fig.2. Routing Evidence Generation Phase

IV.RELATED WORK

In paper "Trustworthiness Management in the Social Internet of Things", IEEE Transactions On Knowledge And Data Engineering, May 2014, M. Nitti, R. Girau, and L. Atzori,[1] focused on how the information provided by members of the social IoT to build a reliable system on the basis of the behavior of the objects. The author proposed two model for the trustworthiness management such as subjective and objective model.

In paper "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions on Parallel and Distributed Systems, Jan 2014, Haojin Zhu[2] has discussed that a malicious and selfish behavior is serious threat routing in delay/disruption tolerant networks (DTNs). The author proposed a probabilistic Trust model for misbehavior detection in order to establish trust among the nodes.

In paper "A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure", IEEE UKSim 15th International Conference on Computer Modelling and Simulation, 2013, H. Banirostam, A. Hedayati, A. Zadeh, and E. Shamsinezhad[3] has discussed about Cloud computing is become an fast growing buzzword, currently not having appropriate tools for their verification of confidentiality, privacy policy, computing accuracy, and

data integrity. Hence author suggested new approach called Trusted Cloud Computing Infrastructure.

In paper "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 2, February 2013, Larry A. Dunning, and Ray Kresman[4] has discussed that in network, in order to sharing of private data among node, assigning secure and unique ID's is required. The authors examine existing and new algorithms for assigning anonymous IDs, with respect to trade-offs between communication and computational requirements.

V. Proposed System

In DTN, information is sent from node to node and this information is sent in the form of packets. When the connection is established, packets are sent from node to node. But in case if connection is lost, data packets are accumulated and then the connection is re-established and data packets are sent again. Thus to avoid packet loss in the network, the method is proposed which is known as a probabilistic misbehaviour detection scheme.

In order to make a proper communication between the sink node and the receiving node and to reduce the high verification cost incurred by routing evidence auditing, a trust model is proposed. In this, a noise is added due to which there will be a packet drop in the network. If there is no drop of packets i.e the data is being sent properly, then that node is considered as a trusted node otherwise it is not. Thus trustworthiness of each node is known.

In the existing terminology, system creates a trust model on the basis of packet drop and then finalise the trust of each node. Propose system will first analyse the trust level by generating multiple sample transaction and then finalise the ranking level and also find the performance analysis.

Advantages:
Delay tolerance will increase.
Transmission overhead will reduce.
Detection performance will increase.
Verification cost will reduce.

In the first module, we propose a general misbehavior detection framework that is based on a series of newly introduced data forwarding evidences. The proposed evidence framework not only detect various misbehaviors but also be compatible to various routing protocols.

In this module, number of nodes are created and the behaviour of nodes is shown. The node communicates with several different nodes. These nodes may be malicious or selfish nodes. Thus the misbehaviour detection framework will find out whether the node is trusted or not.

VI. Conclusion

In this paper, we propose a probabilistic misbehavior detection scheme, which could reduce the transmission overhead. It will reduces the high verification cost incurred by routing evidence auditing. We introduce a probabilistic misbehavior scheme which allows the trusted authority to launch the misbehavior detection at a certain probability. Our simulation results confirm that trust model will increase the detection performance and detect the malicious nodes effectively. Our future work will focus on the extension of trust to other kinds of network.

References

[1] Michele Nitti, Roberto Girau, and Luigi Atzori, "Trustworthiness Management in the Social Internet of Things", IEEE Transactions On Knowledge And Data Engineering, May 2014.

[2] HaojinZhu, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions On Parallel And Distributed Systems, Jan 2014.

[3] Hamid Banirostam, AlirezaHedayati, Ahmad Zadeh, and Elham Shamsinezhad, "A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure", IEEE UKSim 15th International Conference on Computer Modelling and Simulation, March 2013.

[4] Larry A. Dunning, and Ray Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 2, February 2013.

[5] Ramya, P. Basith, "Design of an efficient Weighted Trust Evaluation System for Wireless Sensor Networks", International journal of engineering and computer science, Vol. 3, February 2014.

[6] Jinfang Jiang, Feng Wang, "An efficient distributed trust model for wireless sensor network", IEEE transaction on efficient and distributed system, March 2014.