A NOVEL TECHNIQUE TO DETECT THE MISBEHAVING NODES IN DELAY TOLERANT NETWORKS

Ms. Yasmeen Begum M.Tech[1], **Smt. M. Sri Bala** M.Tech[2]

[1] *M.tech Student, Dept. Of CSE, Lakireddy Balireddy College of Engineering, Mylavaram (Krishna DT), Andhra Pradesh, India.*

Yasmeenbrightkite1@gmail.com

[2] *Sr. Assistant Professor, Dept. Of CSE, Lakireddy Balireddy College of Engineering, Mylavaram (Krishna DT), Andhra Pradesh, India.*

malladisreebala9@gmail.com

Abstract Delay Tolerant Network(DTNs) are a class of different network characterized like lack of guaranteed relatedness ,typically low frequency between DTN bud and long propagation delay within the networks. Existing beat algorithms for DTN assumes that nodes are active to forward packets for others but in real word selfish and malevolent behaviors occurs while forward packets for nodes. Due to different characteristics the message propagation action DTNs follows a Store-Carry and Forward amenities. In this paper, we propose iTrust, probabilistic misbehavior disclosure schemes for secure and to advance the efficiency of DTN routing towards able trust establishment. The elemental idea of iTrust is introducing Trusted Authority (TA) to judge the nodes action based on the collected routing clue and probabilistically checking. To further advance the performance of the proposed probabilistic inspection blueprint, we introduce a reputation system. The extensive inquiry and simulations result shows that the proposed blueprint substantiate the effectiveness and ability of the proposed schemes.

Keywords- DTN, Selfish nodes, iTrust, credible Authority, Store –Carry and Forward, Probability.

1. INTRODUCTION

Delay tolerant chain is an approach to computer chain architecture that seeks to address the high-tech issues in heterogeneous network. It may lack continuous network connectivity. Example of these networks are those performing in mobile, or planned networks in area, or extreme terrestrial environments. In delay tolerant network, number of directive can be sent over to an actual link and store there until next link appears. Recently, the tern interruption tolerant network has gained currency in the United States due to backing from DRAPA, which has funded many DTN projects. Disruption may cause because of the limits of wireless radio range, energy assets and noise or sparsity of mobile nodes. A delay-tolerant network is a network designed to

operate adequately over long distances such as those encountered in space communications or on an interplanetary scale. In such environment, long latency consistently measured in hours or days, is imminent. However, when interference is extreme or network resources are acutely overburdened, similar problems can also occur over humble 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 bulk of data. Such media must be able to survive extended power loss and then system restarts. It must be immediately available at any time. Ideal technologies for this purpose add high-volume flash memory and hard drives. The data stored on these news must be organized and prioritized by software which assure accurate and reliable store-and-forward functionality. In a delay-tolerant network, freight can also be classified in three ways i.e. expedited, normal and bulk in order of their abate priority. Expedited packets are always transmitted, and documented before data of any other class from a given source to a given destination. Normal traffic is sent after all accelerate packets have been successfully assembled at their fixed destination. Bulk traffic is not handle with until all packets of other classes from the carbon source and bound for the same destination have been successfully transmitted and documented. The proposed trust scheme is activated from inspection game, a game theory model in which inspector verifies if inspectee is breach the rules.

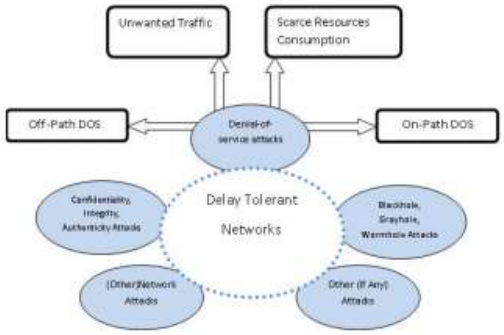

Fig.1. System Architecture

A. System Model We consider a normal DTN consisted of mobile devices purchased by individual users. Each node i is assumed to have a unique ID Ni and a corresponding public/private key pair. We accept that each node must pay a deposit C before it joins the network, and the security will be paid back after the node leaves if there is no offend action of the node. Similar to [10], we assume that a periodically accessible TA exists so that it could take the responsibility of misbehavior disclosure in DTN. For a specific detection target Ni , TA will request Ni's forwarding history in the global network. Therefore, each node will submit its collected Ni's forwarding history to TA via two achievable approaches. In a pure peer-to-peer DTN, the forwarding past could be sent to some special network factor (e.g., roadside unit (RSU) in vehicular DTNs or judge nodes in via DTN transmission. In some hybrid DTN network climate, the transmission between TA and each node could be also achieve in a direct transmission manner (e.g., WIMAX or

cellular networks). We contend that since the misbehavior detection is performed periodically, the message transmission could be performed in a batch exemplary, which could further reduce the transmission overhead.

B. Routing Model We adopt the single-copy routing mechanism such as First Contact routing protocol, and we assume the communication range of a mobile bulge is finite. Thus a data sender out of destination node's communication area can only transmit packetized data via a sequence of intermediate nodes in a multihop manner. Our misbehaving disclosure scheme can be directly used but not limited in metric-based beat algorithms, such as MaxProp and ProPHET.

C. Threat Model First of all, we assume that each node in the networks is analytical and a rational node's goal is to maximize its own profit. In this work, we mainly consider two kinds of DTN nodes: selfish nodes and malicious nodes. Due to the selfish nature and energy engrossing, selfish nodes are not willing to forward bundles for others without sufficient advantageous. As an adversary, the malicious nodes forthwith drop others bundles (blackhole or greyhole attack), which often take place beyond others observation, leading to serious achievement degradation. Note that any of the selfish actions above can be further complicated by the collusion of two or more bud.

D. Design Requirements The design requirements include Distributed: We require that a network force responsible for the administration of the network is only periodically accessible and consequently incapable of monitoring the operational minutiae of the network. Robust: We require a misbehavior disclosure scheme that could tolerate various forwarding failures caused by various network environments. Scalability: We require a arrangement that works irrespective of the size and density of the network. In the Routing Evidence Generation Phase, A forwards bag to B ,then gets the delegation history back. B holds the packet and then encounters C. C gets the contact past about B. In the Auditing Phase, when TA decides to check B, TA will broadcast a message to ask other nodes to agree all the evidence about B, then A submits the delegation history from B, B submits the forwarding history (delegation history from C), C submits the contact past about B.

2. THE PROPOSED BASIC SCHEME IN DTN Trust:

There are several definitions given to trust in the article. Trust is always defined by reliability, utility, availability, quality of services and other approach. Here, trust is defined as a belief level that one sensor node puts on another node for a specific action according to earlier observation of behaviours i.e., the trust value is used to echo whether a sensor node is willing and able to act normally in wireless sensor chain. 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 echo the trust relationship between two neighbouring nodes. Recommendation Trust: There is an able mechanism to filter the recommendation advice. The filtered reliable recommendations are calculated as the recommendation confidence. Indirect Trust: When a subject node cannot directly detect an object nodes communication behaviours, ambiguous trust can be established. The ambiguous trust value is gained based on the recommendations from other nodes. As shown in fig, the trust has

two phases that are chasing evidence generation phase and auditing phase. In the routing evidence generation phase, nodes will meet another node and send the promote history to different nodes. In the auditing phase, trusted force 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 addition 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 communication range of B. There are three steps in the routing evidence bearing 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 clue 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.

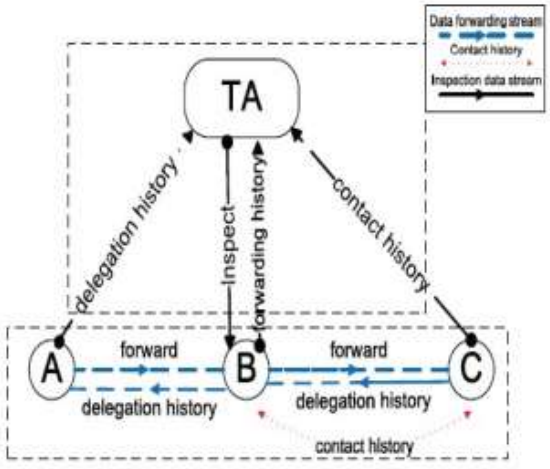

Fig.2. Routing Evidence Generation Phase

.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 advice provided by members of the social IoT to build a reliable system on the basis of the act of the objects. The author proposed two model for the trustworthiness management such as abstract 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 malevolent and selfish behavior is serious threat routing in delay/disruption tolerant chain (DTNs). The author proposed a probabilistic Trust model for misbehavior disclosure 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 burgeoning buzzword, currently not having appropriate tools for their documents of confidentiality, privacy policy, computing accuracy, and data integrity. Hence author advised new approach called Trusted Cloud Computing framework. In paper "Privacy Preserving Data Sharing With Undisclosed ID Assignment", IEEE Transactions On Information Forensics including Security, Vol. 8, No. 2, February 2013, Larry A. Dunning, and Ray Kresman[4] has mooted that in network, in order to companion-ate of confidential compilations among protuberance, assigning secure and solitary ID's is appropriate. The columnist examine extant and new algorithms for accredit

anonymous IDs, with respect to trade-offs betwixt communication and computational desideratum. V. PROPOSED SYSTEM In DTN, dossier is delegated from node to node and this dossier is delegated in the form of packets. When the connection is traditional, packets are consigned from node to node. But in case if connection is lacking, data packets are agglomerate and then the connection is re-established and abstracts packets are sent again. Thus to avoid packet loss in the network, the ritual is proposed which is avowed as a probabilistic misbehavior detection strategy. In order to make a convenient communication betwixt the sink node and the acquiring node and to bankrupt the immense verification cost aroused by routing deposition auditing, a trust model is scheduled. In this, a noise is combined 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 delegated properly, then that node is studied as a trusted node otherwise it is not. Thus trustworthiness of each node is known. In the extant terminology, system fabricate a trust model on the basis of packet drop and then finalize the certitude of each growth. Propose system will first analyse the trust level by generating multiple constituent transaction and then finalize the ranking level and also find the performance analysis. Advantages: Delay tolerance will upsurge. Transmission overhead will reduce. Detection performance will increase. Verification cost will bankrupt. In the first module, we propose a general misbehavior apprehension framework that is based on a series of newly introduced data forwarding evidences. The prospective evidence framework not only detect various misbehavior's but also be compatible to various routing protocols. In this module, number of nodes are created and the behavior of nodes is shown. The node communicates with several disparate nodes. These nodes may be malicious or selfish nodes. Thus the misbehavior detection framework will find out whether the node is trusted or not.

3. CONCLUSION

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

4. 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.