International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

Detecting Misbehavior and Establish Trust Authority in DTN

S.Karthika, MIET Engineering College, TamilNadu, India

Abstract— **Delay/Disruption Tolerant Networks (DTNs) is one of the important areas in wireless communication network, where in node sparseness and delays are particularly high in DTN. DTNs are characterized by large end-to-end communication latency and the lack of end-to-end path from a source to its destination. These characteristics creates several challenges to the security of DTNs. Malicious and selfish behaviors represent a serious threat against routing strategy in Delay/Disruption Tolerant Networks (DTNs).Disruption-Tolerant Networks (DTNs) composed of intermittently connected nodes. Malicious nodes within a DTN may attempt to delay or destroy data. Such attacks include dropping data, flooding the network with extra messages, corrupting routing tables, and counterfeiting network acknowledgments. In this work the proposed local and global feedback Schema to prevent the selfish and malicious nodes. Using this schema it is possible to predict the behavior of the node. This Schema could ensure the security of DTN routing at a reduced cost.**

Index Terms— **Delay Tolerant Networks, Malicious Nodes, Local and Global Feedback Schema, Selfish nodes.**

I. INTRODUCTION

Delay tolerant networks [1] or networks with intermittent connectivity networks are wireless mobile ad hoc often where a communication path between a source node and destination node does not exist, either directly or through established routes by intermediate nodes. This situation occurs if the network is sparse and partitioned into several areas due to high mobility, low density nodes or when the network extends over long distances. A DTN is a combination of smaller networks. It is an overlay on top of special-purpose networks, including the Internet. Delay Tolerant Networks (DTNs) are composed of nodes that cooperate with each other to forward data despite connectivity issues, e.g., long and variable delays, high error rates, and intermittent connectivity[2][3]. Due to their characteristics, DTNs are not amenable to traditional routing protocols for Mobile Ad-Hoc Networks (MANETs) [4], like AODV (Ad hoc on demand distance vector). In Vehicular Delay Tolerant Networks (VDTNs) [5] in which vehicles communicate wirelessly with each other on a DTN manner to disseminate messages. Some potential applications are notification of traffic conditions, weather reports, advertisements, and web or email access. Goal of ZebraNet is tracking of Zebras in wildlife. Goal of Inter planetary Network (IPN) is communication between Earth and Mars. DTNs support interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating between the communication protocols of those networks. In providing these functions, DTNs accommodate the mobility and limited power of evolving wireless communication devices. DTNs were originally developed for interplanetary use, where the speed of light can seem slow and delay-tolerance is the greatest need. However, DTNs may have far more diverse applications on Earth, where disruption-tolerance is the greatest need. The potential Earth applications span a broad range of commercial, scientific, military, and public-service applications. The environments of DTN are characterized by,

1.1 Intermittent Connectivity: The absence of an end-to-end path between source and destination is called **network partitioning**. In such cases, communication using the TCP/IP protocols does not work.

1.2 Long or Variable Delay: In addition to intermittent connectivity, long propagation delays between nodes and variable queuing delays at nodes contribute to end-to-end path delays that can defeat Internet protocols and applications that rely on quick return of acknowledgements or data.

1.3 High Error Rates: Bit errors on links require correction (which requires more bits and more processing) or retransmission of the entire packet (which results in more network traffic). For a given link-error rate, fewer retransmissions are needed for hop-by-hop retransmission than for Internet-type end to-end retransmission (linear increase vs. exponential increase, per hop).

DTN routing protocols use a store, carry and forward approach, which implies some degree of cooperation among nodes, as nodes route other nodes' messages, or pick them in one place and deliver them in another. In order to overcome the lack of end-to-end paths, the protocols replicate messages, if necessary, in each contact. DTN support communication between intermittently connected nodes by isolating delay and disruptions with a store-and-forward technique. The intermittent connectivity may be opportunistic or scheduled contacts.

In DTN attacks are done by selfish nodes and malicious nodes. Selfishness can be termed as a node that doesn't perform its duty. Selfishness in our context can be expressed in two ways. First nodes may deny copying and storing data, which are of no interest to them and destined to a third node. Secondly even if they accept to acquire such data, they may refuse to infect another node with them, i.e. relay data to other nodes. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities).

Routing misbehavior [6] can be caused by selfish (or rational) nodes that try to maximize their own benefits byenjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks. Malicious Nodes are creating attacks by dropping packets to launch an attack. These malicious and selfish nodes can infect the network by inducing some type of attacks.

1.4 Black hole attack– a node can announce itself as having the shortest path to all other nodes, thus it disrupts existing routes and attracts much traffic. Getting a large amount of data leads to new opportunities like selectively forwarding or dropping packets (sometimes called grey hole) or various kinds of traffic and content analysis.

1.5 Wormhole– collaborating attackers can create two or more black holes and connect them

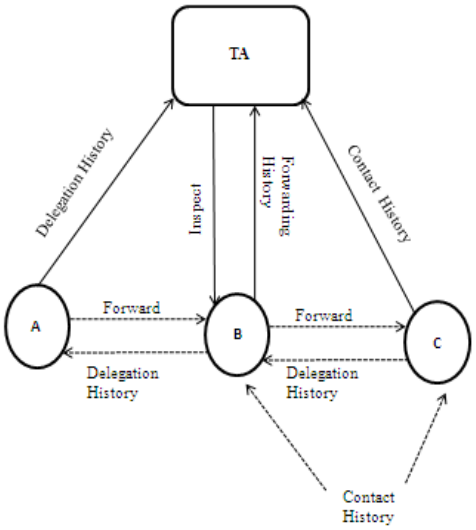


Fig No: 1 System Architecture

A. RELATED WORK

B. Routing Algorithm

Routing in delay-tolerant networking concerns itself with the ability to transport or route, data from a source to a destination, which is a fundamental ability all communication networks must have. Delay and Disruption Tolerant Network characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. In these challenging environments, popular ad hoc routing protocols such as **AODV** and **DSR** fail to establish routes.

2.1PROPHET ROUTING ALGORITHM

PROPHET [7] stands for Probabilistic Routing Protocol using History of Encounters and Transitivity. Real users move in a predictable fashion rather than randomly. Forwarding decision is based on a probabilistic metric called **delivery predictability ($P_{(a,b)}$)** that is set up at every node *a* for each known destination **b.**

Delivery Predictability Calculation

- Updated every time a node is encountered
  $P_{(a,b)} = P_{(a,b)old} + (1 - P_{(a,b)old}) * P_{init}$
- Aged after every time unit (γ is the aging constant.)
  $P_{(a,b)} = P_{(a,b)old} * \gamma^{k}$
- Impact of transitive property on deliver predictability
  $P_{(a,c)} = P_{(a,c)old} + (1 - P_{(a,c)old}) * P_{(a,b)} * P_{(b,c)} * \beta$

Message Forwarding Strategies

Message is transferred if the delivery predictability of the destination of the message is higher at other node.

2.2 MAXPROP ROUTING ALGORITHM

MaxProp [8] uses acknowledgments that are propagated network-wide, and not just to the source. Finally, MaxProp stores a list of previous intermediaries to prevent data from propagating twice to the same node. The MaxProp protocol uses several mechanisms in concert to increase the delivery rate and lower latency of delivered packets. MaxProp uses several mechanisms to define the order in which packets are transmitted and deleted. MaxProp protocol is a ranked list of the peer's stored packets based on a cost assigned to each destination. The cost is an estimate of delivery likelihood. In addition, MaxProp uses acknowledgments sent to all peers to notify them of packet deliveries. MaxProp assigns a higher priority to new packets, and it also attempts to prevent reception of the same packet twice.

3. MISBEHAVING DETECTION SCHEMES

3.1 Credit based Incentive Scheme:

Credit-based schemes [9] introduce some form of virtual currency to regulate the packet forwarding relationships among different nodes. First, a common assumption adopted in existing incentive schemes is that a full end-to-end path between the source and the destination can be determined before data forwarding occurs. This assumption does not hold in DTNs due to its intrinsic opportunistic forwarding nature. Second, the reported schemes are mainly designed for single-copy forwarding. However, multi copy forwarding or even flooding is often adopted to enhance the reliability of DTN communication which makes most existing incentive schemes incompatible with diverse DTN routing.

3.2 Reputation based Incentive Scheme:

Reputation based schemes rely on individual nodes to monitor neighboring nodes' traffic and keep track of each others' reputation so that uncooperative nodes are eventually detected and excluded from the networks.

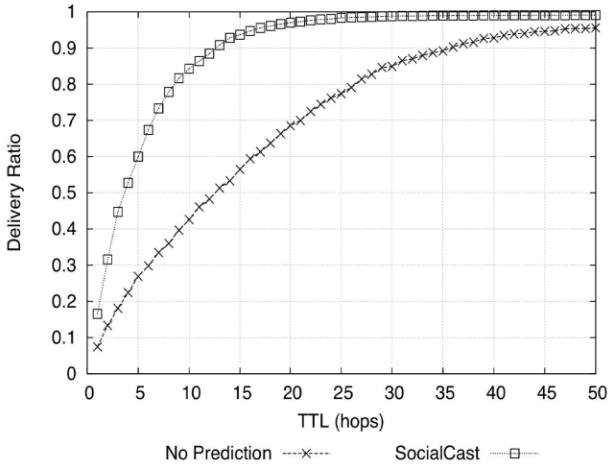
3.3 Trusted Authority

The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. iTrust as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. iTrust introduces a periodically available Trust Authority (TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then TA could punish or compensate the node based on its behaviors.

4. Local and Global Feedback Schema

Trust level of the node is created using the local and global feedback schema. Using the feedback schema it is possible to predict the behavior of the node. Locally and globally the feedback details of the nodes are maintained in a table. Using this, the entering nodes are getting aware of the other nodes. Preventing the nodes from malicious and selfish behavior is possible.

RESULTS



5. CONCLUSION

In DTN using this feedback schema preventing from malicious and selfish nodes are possible. Compared to previous mechanisms transmission overhead is decreased. Packet loss ratio also decreased. Misbehavior detection cost is reduced. Packet delivery ratio is increased.

REFERENCES

[1]"Implementing Delay Tolerant Networking" IRB-TR-04-020, Dec.28 2004 , Michael Demmer, Eric Brewer, Kevin Fall, Sushant Jain, Melissa Ho, Robin Patra.

[2]"Routing in Wireless Networks with Intermittent Connectivity" Cardei, C.Liu and J.Wu,Florida Atlantic University Boca Raton, Florida ,U.S.A.

[3] A. Lindgren and A. Doria." Probabilistic Routing Protocol for Intermittently Connected Networks." draft-lindgren-dtnrg-prophet-03, 2007.

[4]" MANET: Vulnerabilities, Challenges, Attacks, Application" Priyanka Goyal, Vinti Parmar, Rahul Rishi.

[5] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots", in Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 19-25, 2009.

[6] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012.

[7] A. Lindgren and A. Doria." Probabilistic Routing Protocol for Intermittently Connected Networks." draft-lindgren-dtnrg-prophet-03, 2007.

[8] J. Burgess, B. Gallagher, D. Jensen and B. Levine. "Maxprop: Routing for vehicle-based disruption-tolerant networks." In Proc. of IEEE INFOCOM'06, 2006.

[9] B. B. Chen, M. C. Chan,"Mobicent:a Credit-Based Incentive System for Disruption Tolerant Network" in IEEE INFOCOM'2010.