International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Misbehavior Detection Embedded with Agent Based Routing in Delay Tolerant Networks

K.Deepika[1], Sujatha S G[2]

1M. Tech in Computer Science, CMR Institute of technology, Bangalore, India

[2]Assistant Professor, CMR Institute of Technology, Bangalore, India

Abstract: ***In a Delay Tolerant Networks depend Routing schemes depends on the intermediate nodes to carry messages till the destination. Intermediate node forwards the messages to other nodes till the destination. Malicious and selfish behaviors represent a serious threat against routing in Delay Tolerant Networks so it may decrease the performance of network. Thus, efficient and faster spreading of messages and the selfish node detection is essential to reduce the delay of sending a message from source to destination. In this paper, we aim to design a new agent aided routing scheme to avoid large message delivery delay and detection of selfish node to increase the performance in Delay Tolerant Networks. Here, the source of a message is permitted to create unlimited copies of a message and distribute these copies to agents. Agents acting as the representative of the sources receive messages from the sources based on their node visited list and delivery predictability. After that, the agents forward the copies to the other neighboring agents. Thus, the agents help in faster and efficient dissemination of a message in the network which helps in reducing message delivery delay. Misbehavior detection scheme, for secure DTN routing toward efficient trust establishment. For detection of selfish node 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. The extensive analysis and simulation results demonstrate the effectiveness and efficiency of the proposed scheme.***

Keywords: Delay tolerant networks, Selfish node, Agents, iTrust, Trusted Authority

1. Introduction

DELAY tolerant networks (DTNs) as shown in fig 1, such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information) [1], and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion.

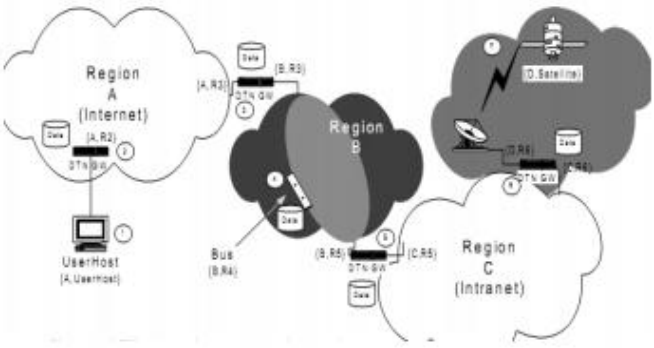

Figure 1: Architecture of Delay Tolerant networks

Characteristics of Delay Tolerant networks

- **Intermittent Connection**
  As the node's mobility and energy are limited, DTN frequently disconnects, thus resulting in continue change in DTN topology. That is to say, the network keeps the status of intermittent connection and partial connection so that there is no guarantee to achieve end-to-end route.
- **High delay, low efficiency, and high queue delay**
  End-to-end delay indicates that the sum of the total delay of each hop on the route. The delay is consisted of waiting time, queuing time, and transmission time [1]. Each hop delay might be very high due to the fact that DTN intermittent connection keeps unreachable in a very long time and thus further leading to a lower data rate and showing the asymmetric features in up-down link data rate. In addition, queuing delay plays a main role in end-to-end delay and frequent fragmentations in DTN make queuing delay increasing.
- **Limited resource**
  Node's computing and processing ability, communication ability and storage space is weaker than the function of an ordinary computer due to the constraints of price, volume and power. In addition, the limited storage space resulted in higher packet loss rate.
- **Limited Life time of node**
  In some special circumstances of the restricted network, the node is common to use the battery power on the state of hostile environment or in harsh conditions, which will cut the life time of node. When the power is off, then the node cannot guarantee normal work. That is to say, it is very possible the power is off when the message is being transmitted.
- **Dynamic topology**
  Note that the DTN topology is dynamic changing for some reasons such as environmental changes, energy depletion or other failures, which results in dropping out of network. Or, the requirements of entering DTN also make topology change.
- **Poor Security**
  In general, DTN is vulnerable to--besides threats of wireless communication network--eavesdropping,

message modification, routing spoofing, Denial of Service (DoS), and other security threats, etc, due to the lack of specialized services and maintenance in real-world.

- **Heterogeneous interconnection**
  DTN is an overlay network for transmission of asynchronous message. Introducing the bundle layer, the
- DTN can run on different heterogeneous network protocol stacks and DTN gateway ensures the reliable transmission of interconnection message.

Applications

- **Deep Space Networking**
  The DINET I, known as Deep Impact Network is an experimental validation of Inter – Planetary Networks, which is the NASA's implementation of Delay – Tolerant Networks. NASA (National Aeronautics & Space Administration) has successfully tested the first deep space communication network model using the DTN by transmitting around 200 space images (approx 14 MB) to and from a space craft known as EPOXI – uploaded with DTN software (functioned as a DTN router,) located more than 32 million kilometers from earth.
- **Tactical Military Applications**
  With gradual deepening and development of modern military warfare towards Network Centric Warfare (NCW), he performance of Networks and Protocols will play a significant role. The custom network protocols based on end – to – end connectivity is not suited for military communication networks, which is a long/variable delay with high error rates and greatly heterogeneous. Realization of a robust, intelligent and integrated communication and careful consideration of types of assets that have to be connected will form a solid foundation for Network Centric Warfare
- **Underwater/Acoustic Networking**
  The underwater acoustic networks are generally formed by acoustically connected ocean – bottom Sensors, autonomous underwater vehicles & surface stations which provide links to on – shore control centre.
- **Smartphone Application**
  The Delay Tolerant Network Approach can be implemented in the Android platform to provide connectivity in environments that lack Efficient Network Infrastructures.

In this paper, we have proposed a new Agent Aided Routing scheme and propose iTrust. The idea of our routing scheme is as follows: first we allow a source to generate unlimited copies of a message. Then we allow the source to forward one or more copies of the message to the agents based on the visited list and delivery predictability of the agent. An agent is a node that meets the source directly. We then propose each agent to spread the message by forwarding only a single copy of the message to each node seen. The nodes carry the message until the destination is met and once found it delivers the message directly to the destination. In this way our agents help in efficient and faster spreading of messages they receive from the sources. Simulation results show that the proposed scheme, the Agent propose iTrust, a probabilistic misbehavior detection scheme to achieve efficient trust establishment in DTNs

2. Related Work

Despite of the challenges of routing in DTN many routing schemes have been reported in the literature. Some of the routing schemes inject multiple copies of a message into the network and achieve higher delivery ratio and lower delay, and they are known as replication based routing schemes. But due to redundant copies of messages, these schemes consume network resources like buffer space, bandwidth and energy [5]. Replication based schemes like Epidemic [6], PROPHET [7] MaxProp [8], RAPID [9], PREP [10] etc. are considered into the category of flooding based schemes, because these schemes replicate as many copies of a message as the network permits which is vulnerable to high network contention and could lead to huge overhead and latency. Spray and Wait [1], ORWAR [11], Spray and Focus [12], and EBR [13] are Quota based schemes which relay limited number of copies of a message in the network to save the network resources. Spray and Wait (SW) [1] makes use of two phases;

Spray phase and Wait phase. Initially in this scheme, L number of copies of a message is generated by the source node. The source node forwards the L copies of a message to L nodes which do not have a copy of the message during the spray phase. If the destination is not among these L nodes, then the scheme switches to the Wait phase. In the Wait phase the L nodes hold their copy of the message until they reach to the destination. By improving the spray phase of SW, Binary Spray and Wait (BSW) [1] routing scheme has been evolved. During the spray phase of BSW routing scheme, a node forwards half the copies of a message, till it has more than one copy of that particular message, to a node that does not have a copy of the message. The node switches to the Wait phase when it is left ith only a single copy of the message. Node performs direct transmission when it meets the destination.

In PROPHET [7], each node forwards a message to its destination node using delivery predictability. When two nodes meet, the node with the more delivery predictability of the desired destination wins the message destined for that destination. However, PROPHET has higher average delay when nodes have low buffer size. Also it experiences high overhead because the average number of forwarded messages is high here. Another replication based routing technique, Epidemic [6] routing, is flooding based in nature. In this routing scheme, nodes continuously replicate and transmit messages to newly discovered contacts that do not already possess a copy of the message.

3. Proposed System

Delay tolerant networks depend on the intermediate nodes to carry messages; hence there is a need for efficient and faster spreading of messages to reduce the delay of sending a msg. This scheme can be briefly explained in three process

- **Generation and Forwarding**: The source node utilizes the visited list and delivery predictability of an agent to decide the number of copies of a message the agent should receive from it. The agents act as representative of the source.

- **Replication:** Agent will replicate a copy of a message to each node that does not posses it till the agent has more than one copy remaining.
- **Detection of selfish node:** propose iTrust, a probabilistic misbehavior detection scheme to achieve efficient trust establishment in DTNs

A. The Source and the Agent

A source is a node that wants to convey some messages to their particular destinations. To spread a message in the network quickly and to create more agents we do not impose any limit on the number of copies a source can generate. A source can send messages to multiple agents and it can work as an agent for other sources as well. An agent is an intermediate node which meets the source directly i.e. the first hop of a source. An agent receives one or more copies of a message from the source. Based on the number of nodes visited by the agent and the delivery predictability of the agent for the destination of that message, the source gives one or more copies to the agent. An agent with more than one copy of a message can replicate a copy to a node lacking the message. A node working as the agent for other sources acts as the source for messages generated by the node itself.

B. Visited List of a Node

We allow each node to keep a list of nodes it has visited throughout the lifetime of the network. We use the set Vi to represent the visited list of node i. If we have n number of nodes in the network then at certain instance of time Vi can be represented using

Vi ⊆ N

Where N is the set of (n - 1) nodes in the network

C. Delivery Predictability of an Agent

Similar to PROPHET [7], we calculate the delivery predictability, P(b) [0,1] a,b ∈ , in each node A for each known destination B. The delivery predictability indicates the likelihood of node A delivering a message to a particular destination B. When two nodes encounter each other, we permit the nodes to exchange the P-values of their known destinations and use the information to update the delivery predictability information at both ends. Thus, when a source meets an agent we use the P values of the agent to determine the number of copies of the message it should receive from the source node.

D. Agent Copy Determination

We permit a source node to generate unlimited copies of a message and disseminate these copies to the agents based on their visited lists and delivery predictabilities. When a source node S, carrying a message M with unlimited copies for a destination D, meets an agent A, we allow the source S to use

If cs(s,a) = 0, for an agent then the source forwards a single copy of a message to the agent for the fastest spreading. An agent visiting more nodes throughout the network lifetime and having good delivery predictability for the destination of a message is a better customer or steward to receive and carry more copies of the message.

E. Spreading of Messages by an Agent

Whenever an agent carrying more than one copy of a message meets a new node lacking the message, we permit the agent to forward a single copy of the message to the node. When the copy number of a message in an agent reaches one we compel the agent to stop forwarding or spreading the message. Having a single copy of a message an agent waits for the destination, if found, delivers the message to its destination. Thus, an agent, acting as the representative of a source, helps in faster and efficient spreading of a message which may reduce the message delivery delay. An intermediate node carrying a single copy of a message can only deliver a message to its final destination.

F. Detection of Selfish node:

In this process, we define three kinds of data forwarding evidences that could be used to judge if a node is a malicious one or not.

Delegation task evidence

Suppose that source node N_{src} is going to send a message M to the destination N_{dst}. Without loss of generality, we assume the message is stored at an intermediate node Ni, which will follow a specific routing protocol to forward M to the next hop. When N_j arrives at the transmission range of Ni, Ni will determine if N_j is the suitable next hop, which is indicated by flag bit flag. If N_j is the chosen next hop (or flag ¼ 1), a delegation task evidence IEi!j task needs to be generated to demonstrate that a new task has been delegated from Ni to Nj.

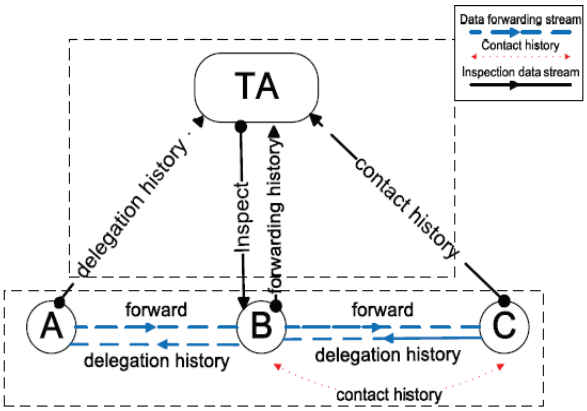

Figure 2: Routing evidence generation phase

Forwarding history evidence:

When N_j meets the next intermediate node N_k, N_j will check if N_k is the desirable next intermediate node in terms of a specific routing protocol. If yes (or flag ¼ 1), N_j will forward the packets to N_k, who will generate a forwarding history evidence to demonstrate that Nj has successfully finished the demonstrate the authenticity of forwarding history evidence.

Contact history evidence: Whenever two nodes N_j and N_k meet, a new contact history evidence will be generated as the evidence of the presence of N_j and N_k. Based on the above three evidences misbehavior detection algorithm is run. The output of it determines whether a particular node is selfish or not. After which the node is blacklisted from the forwarding process. Also, the selfish here are punished by

reducing their reputation score (iTrust) and cooperative nodes are rewarded.

4. Simulation Results

Scenario 1:

Figure 3: Graph for Throughput

Above Scenario shows that at the start the throughput will increase later it will decrease by exponential.

Scenario 2:

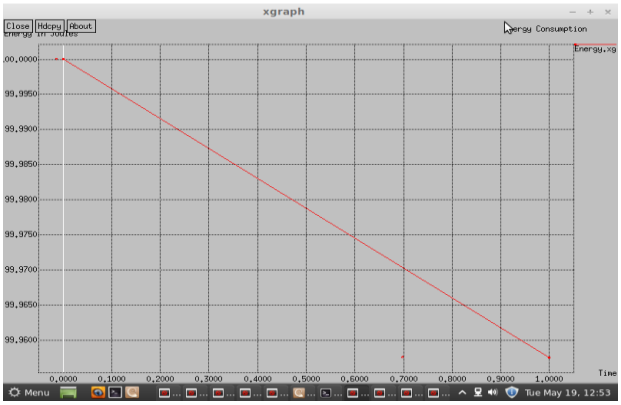

Figure 4: Graph for Energy Consumption

The above graph shows power consumption decrease exponentially.

Scenario 3:

Figure 5: Graph for packet drop

Packet drop increases later decreases exponentially.

5. Conclusion and Future Enhancement

In this work, we have designed a new agent aided routing scheme for Delay Tolerant Networks. Based on these three evidences collected we run the misbehavior detection algorithm to find whether a node is misbehaving or not. If found misbehaving in order to achieve cooperation among nodes we reward or punish the nodes. And finally only the well behaved nodes are chosen to forward the message. This way we reduce the overhead and also bring out cooperation among nodes. The graph shown is for transmission of one message. Thus, our main contribution is that we proposed to reduce the message delivery delay by spreading the messages faster and efficiently. Thus, we allow sources to forward only necessary number of copies of a message to the agents to keep the overhead as less as possible and increase the delivery and delay performance. In future we can use different selfish node detection technique.

References

[1] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, “Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks,” Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-tolerant Networking, USA, pp. 252-259, August 2005

[2] W. Zhao, “Routing and network Design in Delay Tolerant Networks”, Submitted in partial fulfillment for the degree of Doctor of Philosophy, College of Computing, Georgia Institute of Technology, 2006.

[3] M. A. T. Prodhan, R. Das, M H. Kabir, G. C. Shoja, “TTL Based Routing in Opportunistic Networks,” Journal of Network and Computer Applications, vol. 34, issue 5, pp. 1660-1670, September 2011.

[4] E Bulut, “Opportunistic Routing Algorithms in Delay Tolerant Networks”, Submitted in partial fulfillment for the degree of Doctor of Philosophy, Rensselaer Polytechnic Institute Troy, New York, February, 2011.

[5] J. Zhang, G. Luo, “Adaptive Spraying for Routing in Delay Tolerant Networks,” Wireless Pervasive Communication, Springer, May 2011..

[6] Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks", Technical Report CS-20OO06, Duke University, April 2000

[7] K A. Lindgren, A. Doria, and O. Schelen, “Pobabilistic Routing in Intermittently Connected Networks,” SIGMOBILE Mobile Computing Communications Review, vol. 7, no. 3, pp. 19-20, July 2003.

[8] J. Burgess, B. Gallagher, D. Jensen, and B. N. Levine, “Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks,” INFOCOM, pp. 1-11. IEEE, April 2006.

[9] Balasubramanian, B. Levine, and A. Venkataramani, “Dtn Routing as a Resource Allocation Problem,” SIGCOMM Computing Communications Review., vol. 37, no. 44, pp. 373-384, August 2007.

[10] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain, and R. Krishnan, “Prioritized Epidemic Routing for Opportunistic Networks,” Proceedings of the 1st

international MobiSys Workshop on Mobile Opportunistic Networking, USA, pp. 62-66, June 2007.
[11] G. Sandulescu and S. Nadjm-Tehrani, "Opportunistic DTN Routing with Window-Aware Adaptive Replication," Proceedings of the 4th Asian Conference on Internet Engineering, USA, pp. 103-112, November 2008.
[12] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and Focus: Efficient Mobility-Assisted Routing for Heterogeneous and Correlated Mobility," Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications Workshops, USA, pp. 79- 85, March 2007.
[13] S. C. Nelson, M. Bakht, and R. Kravets, "Encounter-Based Routing in DTNs," INFOCOM, pp. 846-854, April 2009.
[14] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay-Tolerant Networks," Proc. Military Comm. Conf. (Milcom '10), 2010.
[15] Haojin Zhu, Mianxiong Dong "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks" ieee transactions on parallel and distributed systems, vol. 25, no. 1, january 2014
[16] Shahid Md. Asif Iqbal#, Alok Kumar Chowdhury #, Amina Akhter "AAR: Agent Aided Routing for Faster and Efficient Spreading of Messages in Delay Tolerant Networks"