SELF RECOGNITION OF ROUTING MISBEHAVIOUR IN DISRUPTION TOLERANT NETWORKS

K.Prasanth Kumar[1],S.Oviya[2],J.Rajasekar[3],S.Sathish Kumar[4]
[1,2,3] Student, B.E CSE, SNS College of Technology, Coimbatore, TamilNadu.
[4] Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, TamilNadu.

Abstract— A Disruption tolerant networks is a network designed temporary, have the unique features of intermittent connectivity which makes routing quite different from other wireless network. Routing misbehavior like selfish or malicious node can cause packet delay and modifying packets in a network. A node is required to keep a few signed contact record of its previous contact based on it the next node can detect a packet dropping,although here it may reduces the packet delivery ratio and waste the system resources such as power and bandwidth. To reduce this problem we propose a scheme as record handler, it is used to maintain the entire information about packet separately and to provide more security and we introduce RC4 algorithm where the message and the key can be send individual to nodes for avoiding misbehaviour on a network.

Index Terms— Disruption Tolerant Networks, Routing misbehavior, Mitigation.

1 INTRODUCTION

Disruption **T**olerant **N**etworking is a networking architecture that is designed to provide communications in the most unstable and stressed environments, where the network would normally be subject to frequent and long lasting disruptions and high bit error rates that could severely degrade normal communications.DTN works using different kind of approach than TCP/IP for packet delivery that is more resilient to disruption than TCP/IP. DTN is based on a new experimental protocol called the Bundle Protocol (RFC 5050). BP sits at the application layer of some number of constituent internets, forming a store-and-forward overlay network. The Bundle Protocol (BP) operates as an overlay protocol that links together multiple subnets into a single network. The basic idea behind DTN network is that endpoints aren't always continuously connected. In order to facilitate data transfer, DTN uses a store-and-forward approach across routers that is more disruption-tolerant than TCP/IP. However, the DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity.

Disruption Tolerant Networks are frequently used in disaster relief missions, peace-keeping missions, and in vehicular networks. Most recently NASA has tested DTN technology for spacecraft communications.A disruption-tolerant network (DTN) is a network designed so that temporary or intermittent communications problems, limitations and anomalies have the least possible adverse impact. There are several aspects to the effective design of a DTN, including:

- The use of fault-tolerant methods and technologies.
- The quality of graceful degradation under adverse conditions or extreme traffic loads.
- The ability to prevent or quickly recover from electronic attacks.
- Ability to function with minimal latency even when routes are ill-defined or unreliable.

Fault-tolerant systems are designed so that if a component fails or a network route becomes unusable, a backup component, procedure or route can immediately take its place without loss of service. At the software level, an interface allows the administrator to continuously monitor network traffic at multiple points and locate problems immediately. In hardware, fault tolerance is achieved by component and subsystem redundancy.Graceful degradation has always been important in large networks. One of the original motivations for the development of the Internet by the Advanced Research Projects Agency (ARPA) of the U.S. government was the desire for a large-scale communications network that could resist massive physical as well as electronic attacks including global nuclear war. In graceful degradation, a network or system continues working to some extent even when a large portion of it has been destroyed or rendered inoperative.

Electronic attacks on networks can take the form of viruses, worms, Trojans, spyware and other destructive programs or code. Other common schemes include denial of service attacks and malicious transmission of bulk e-mail or spam with the intent of overwhelming network servers. In some instances, malicious hackers commit acts of identity theft against individual subscribers or groups of subscribers in an attempt to discourage network use. In a DTN, such attacks may not be entirely preventable but their effects are minimized and problems are quickly resolved when they occur. Servers can be provided with antivirus software and individual computers in the system can be protected by programs that detect and remove spyware.

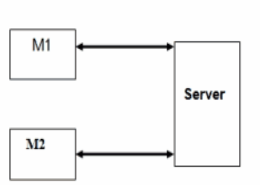
As networks evolve and their usage levels vary, routes can change, sometimes within seconds. This can cause temporary propagation delays and unacceptable latency. In some cases, data transmission is blocked altogether. Internet users may notice this as periods during which some Web sites take a long time to download or do not appear at all. In a DTN, the frequency of events of this sort is kept to a minimum.Routing is the transfer of data packets from one location to another, and it's one of the fundamental network functions.

Network throughput, which is the ratio of data packets sent and received, is directly related to the routing function of any network. In other words, if the routing function is good enough, then we can expect a better output from the network. In today's environment, we see different types of networks.

- *S.Oviya is Final year B.E Computer Science and Engineering in SNS College of Technology,Coimbatore,Tamilnadu,India. E-mail: oviya.vs@gmail.com*
- *K.PrasanthKumar is Final year B.E Computer Science and Engineering in SNS College of Technology. Coimbatore,Tamilnadu,India .E-mail: prasanthkamali@gmail.com*
- *J.RajaSekar is Final year B.E Computer Science and Engineering in SNS College of Technology. Coimbatore,Tamilnadu,India. E-mail: clicktorajasekar@gmail.com*
- *S.SathishKumar is Assistant Professor in Department of Computer Science and Engineering in SNS College of Technology, Coimbtore,Tamilnadu,India.E-mail: sathishkumar2k9@gmail.com*

Figure A shows one type of network, a traditional fixed computer network.

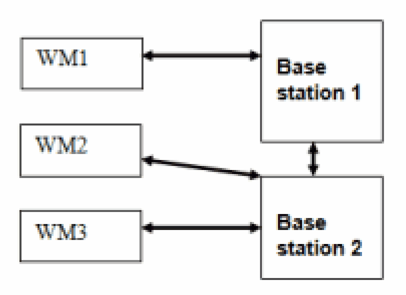
FigureA



Traditional fixed network

Another type of network is a wireless network, which you can see in Figure B. Other than a wireless network, which depends on some sort of supporting structure for normal communication operations, mobile ad-hoc networks are short range wireless network provide communication services without the support of any centralized structure.

FigureB



How wireless networks work

Routing in mobile ad-hoc networks is achieved through mobile nodes acting as intermediate nodes. These nodes are responsible for receiving and forwarding data packets from one host to another in the network. The absence of a fixed infrastructure makes routing a challenge in a mobile ad-hoc environment.There are also several other issues which have an effect on the overall performance of the mobile ad-hoc network. Some of these issues include bandwidth constraints, hidden terminal problems, security and limited battery power of the participating nodes. These issues are somehow interrelated with the overall routing mechanism. In order to gain a better routing solution, it's almost always required to address these issues in conjunction with the routing problem of the mobile ad-hoc network.

Within the traditional routing mechanism, there are also several other issues to consider. For example, a node can become selfish and refuse to forward data packets to other nodes; or the node fails to forward data packets to the destination node. Finally, a node could enter an an inactive state because of a limited power supply. These are some of the issues can result in communication breakdowns and can eventually lead us to an abnormal network environment.Let's consider when a node refuses to forward data packets to the other nodes. There are number of approaches you can take that would solve this problem. These solutions could involve an initial mutual agreement which can force all intermediate nodes to act as intermediate nodes without refusing to forward any data packet which comes to them.

2 EXISTING SYSTEM

Disruption Tolerant Networks (DTNs) exploit the intermittent connectivity between mobile nodes to transfer data. Due to a lack of consistent connectivity, two nodes exchange data only when they move into the transmission range of each other when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards the packet. In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks.

Routing misbehavior will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets.Neighborhood monitoring relies on a connected link between the sender and its neighbor, which most likely will not exist in DTNs Another line of work uses the acknowledgement (ACK) packet sent from the downstream node along the routing path to confirm if the packet has been forwarded by the next hop.Although end-to-end ACK schemes are resistant to such colluding attacks, the ACK packets may be lost due to the opportunistic data delivery in DTNs. where each packet has multiple replicas, it is difficult for the source to verify which replica is acknowledged since there is no persistent routing path between the source and destination in DTNs.

In DTNs, one serious routing misbehavior is the black hole attack, in which a black hole node advertises itself as a perfect relay for all destinations, but drops the packets received from others.Another related attack is the wormhole attack, which has been recently addressed on detecting node clone attacks in sensor networks, since both detect the attacker by identifying some inconsistency. However, our work relies on a different kind of inconsistency in DTNs, and DTNs do not have the reliable link connection used in existing solutions for node clone attacks.

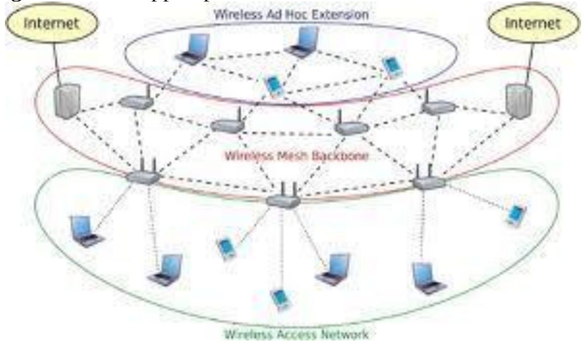
Disadvantage

- A node may misbehave by dropping packets
- Selfish nodes that are unwilling to spend resources
- Malicious nodes that drop packets to launch attacks.
- A misbehavior node can loss the data or drop the received packets.
- In such nodes routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth.

3 PROPOSED SYSTEM

We provide the scheme which detects packet dropping in a distributed manner. In this scheme, a node is required to keep previous signed contact records such as the buffered packets and the packets sent or received, and report them to the next contact node which can detect if the node has dropped packets based on the reported records.Misbehaving nodes may falsify some records to avoid being detected, but this will violate some consistency rules. To detect such inconsistency, a small part of each contact record is disseminated to some selected nodes which can collect appropriate contact records and detect the misbehaving nodes with certain probability we propose a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes.Routing misbehavior has been widely studied in mobile adhoc networks .These works use neighborhood monitoring or acknowledgement (ACK) to detect packet dropping, and avoid the misbehaving nodes in path selection.

Our approach consists of a packet dropping detection scheme and a routing misbehavior mitigation scheme. Contact record during each contact and report its previous contact records to the contacted node. Based on the reported contact records, the contacted node detects if the misbehaving node has dropped packets.



Wireless Networks

The misbehaving node may misreport to hide its misbehavior, but forged records cause inconsistencies which make misreporting detectable. To detect misreporting, the contacted node also randomly selects a certain number of witness nodes for the reported records and sends a summary of each reported record to them when it contacts them.The witness node that collects two inconsistent contact records can detect the misreporting node. Illustrates our approach for routing misbehavior mitigation it reduces the data traffic that flows into misbehaving nodes in two ways:First,if a misbehaving node misreports, it will be blacklisted and will not receive any packet from other nodes;Second,if it reports its contact records honestly, its dropping behavior can be monitored by its contacted nodes, and it will receive much less packets from them.

Advantages

- History of the packet should maintain separately.
- Detect packet dropping.
- limiting the number of packets forwarded to the misbehaving nodes

4 PROBLEM ANALYSIS

In disruption tolerant networks (DTNs), spiteful nodes may collapse received packets. This type of routing misbehavior may diminish the packet delivery proportion and dissipates system resources such as energy and bandwidth. Even though new methods have been anticipated to diminish routing misbehavior in mobile ad hoc networks, they cannot be openly applied to DTNs because of the broken connectivity between the connected nodes. In DTNs, a node may misbehave by dropping packets even when it has adequate buffer. Routing misbehavior can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to commence attacks.

NETWORK CONSTRUCTION

It is developed in order to create a dynamic network. In a network, nodes are interconnected and the resources can be shared among them. For the successful data transfer the network must be properly controlled and handled. This module is designed in order to develop a controlled network traffic environment. Our project aim is to reduce the packet loss during data transmission and find the attacks.

DTN NODES

Disruption Tolerant Network is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space. DTN is required to keep a few signed contact records with mobile nodes. This Previous Records is utilized to verify the trustworthiness of DTN.

RECORDS HANDLER

The Records handler is used to maintain the records of the each and every nodes. The records are all about the data transmission information like size of the packet, time from a particular node to the other nodes. From the Records handler we may able to find data transmission information each node.

WITNESS NODE

A witness node is a node which has some authority to compel testimony to have, knowledge relevant to an event or other matter of interest. The witness node will verify the Original data packets the will be sent via each and every node. So that we can find the Attacker node or the node would give the wrong information.

BUFFER CAPACITY TECHNIQUE

The Buffer Capacity Technique (BCT) is used to find the original buffer capacity of the DTN Nodes. If the capacity of the DTN nodes is mentioned as 20 Mb and the a node is sending the 10 Mb, but it originally handles only 5 Mb. So that we may able to find the capacity of the buffer space easily by using the BCT.

VERIFICATION, COMPARISON AND IDENTIFICATION OF ATTACKS

The Witness node will verify the data packets that are originally send by the Each and Every node. If the data has to be transmitted from A to B. The witness node will calculate the original data packets that was send by the A node using records information that was stored in the Records Handler. So that we can also verify and compare the data packets that were send via each and every node. We're also differentiating genuine traffic packet loss with malicious packet loss by comparing the Buffer level of every node. So that we can also find the attacks very easily.

ENCRYPTION AND DECRYPTION

For security purpose we're encrypting the data packet at the sender end and decrypt it the receiver end. This will provide more security, when the data packets were hacked by the hacker at the time of data transmission. For Encryption we're using RC4 Algorithm.

5 CONCLUSION

In this paper, we presented a scheme to detect packet dropping in DTNs. The detection scheme works in a distributed way i.e., each node detects packet dropping locally based on the collected information. Moreover, the detection scheme can effectively detect misreporting even when some nodes collude. Analytical results on detection probability and detection delay were also presented. Based on our packet dropping detection scheme, we then proposed a scheme to mitigate routing misbehavior in DTNs. The proposed scheme is very generic and it does not rely on any specific routing algorithm. Trace-driven simulations show that our solutions are efficient and can effectively mitigate routing misbehavior.

REFERENCES

[1] Allam Mousa and Ahmad Hamad "Evaluation of the RC4 Algorithm for Data Encryption" in Electrical Engineering Department An-Najah University, Nablus, Palestine.

[2] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in Proc. ACM MobiHoc, 2007, pp.32–40.

[3] H. Yang, J. Shu, X. Meng, and S. Lu, "Scan: Self-organized network layer security in mobile ad hoc networks," IEEE J. Sel. AreasCommun., vol. 24, no. 2, pp. 261–273, 2006.

[4] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550,May 2007.

[5] Q. Li, W. Gao, S. Zhu, and G. Cao, "A routing protocol for socially selfish delay tolerant networks," in Ad Hoc Networks, Aug. 2011, DOI:10.1016/j.adhoc.2011.07.007.

[6] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 2000, pp.255–265.

[7] W. Gao and G. Cao, "On exploiting transient contact patterns for data forwarding in delay tolerant networks," in Proc. IEEE ICNP, 2010, pp.193–202.

[8] W.Gao,Q.Li, B. Zhao, andG. Cao, "Multicasting in delay tolerant networks:A social network perspective," in Proc. ACM

MobiHoc, 2009,pp. 299–308.

[9] W. Gao and G. Cao, “User-centric data dissemination in disruption tolerant networks,” in Proc. IEEE INFOCOM, 2011, pp. 3119–3127.

[10] Y. Xue and K. Nahrstedt, “Providing fault-tolerant ad-hoc routing service in adversarial environments,” Wireless Pers. Commun., vol. 29,no. 3-4, pp. 367–388, 2004.