International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

DETECTING SELFISH ROUTING AND MISBEHAVIOR OF MALICIOUS NODE IN DISRUPTION TOLERANT NETWORKS

Ms.Aarthy D.K.[1], Mr.C.Balakrishnan[2]

[1](PG Scholar) Computer Science &Department, S.A Engineering College, Chennai ,Tamil Nadu;
[2](Assistant Professor) Department of PG Studies, S.A Engineering College, Chennai ,Tamil Nadu.

Email:aarthy13bloom@gmail.com

Abstract

Disruption Tolerant Networks (DTNs) exploit the intermittent connectivity between nodes to transfer data. It follows a store-carry-forward mechanism to transfer data. A node misbehave by dropping packets and acts selfish as they are unwilling to spend resources such as power and buffer on forwarding packets of other nodes. In such nodes routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Methods to mitigate routing misbehavior in mobile ah-hoc networks cannot be applied to DTN because of its intermittent connectivity. Existing systems are designed to identify selfish node or malicious node on DTNs. When it finds misbehaving or packet dropping node then it sends information to server. Server will then stop the data transfer and choose alternate route for communication. Proposed scheme requires each node to maintain a signed communication report (CR). These communication reports are encrypted to avoid forgery. The contact node maintains the communication report that is generated on contacting a node. It detects misbehaving node and is selected dynamically to avoid it being compromised. When a misbehaving node misreports, it is converted to legitimate node so as to avoid the wastage of system resources.

***Keywords*-- Detection; disruption tolerant networks; mitigation; routing misbehavior; security.**

I. INTRODUCTION

DTN, Disruption Tolerant Networking 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 a router 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.

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. Routing misbehavior has been widely studied in mobile ad hoc networks. These works use neighborhood monitoring or acknowledgement (ACK) to detect packet dropping, and avoid the misbehaving nodes in path selection. However, they do not consider the intermittent connectivity in DTNs and cannot be applied to DTNs.

If the nodes in a DTN are controlled by rational entities, such as people or organizations, the nodes can be expected to behave selfishly and attempt to maximize their utilities and conserve their resources. Since routing is an inherently cooperative activity, system operation will be critically impaired unless cooperation is somehow incentivized. The lack of end-to-end paths, high variation in network conditions, and long feedback delay in DTNs imply that existing solutions for mobile ad-hoc networks do not apply to DTNs.

There are several aspects to the effective design of a DTN, including:

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

- 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.

1.1 Network Examples of DTN

Vehicular Networks

- DakNet.
- Message ferry.
- Village network.

Mule Networks

- Zebra net- The goal is tracking of zebras in wildlife.
- Sámi Network Connectivity.
- Carrier Pigeons-RFC 1149, RFC 2549 - Implemented by Bergen Linux users group.

Inter Planetary Networks

- Deep space networks

Sensor Networks

- Acoustic underwater networks

Ad hoc Networks (MANET)

- Military tactical networks

II. EXISTING SYSTEM

In mobile ad hoc networks, much work has been done to detect packet dropping and mitigate routing misbehavior. To detect packet dropping, Marti *et al.* Proposed watchdog-based solutions in which the sending node operates in promiscuous mode and overhears the medium to check if the packet is really sent out by its neighbor. Some follow-up works have used this neighborhood monitoring approach to detect packet dropping. However, neighborhood monitoring relies on a connected link between the sender and its neighbor, which most likely will not exist in DTNs.

In DTNs, a node may move away right after forwarding the packet to its neighbor, and thus cannot overhear if the neighbor forwards the packet. 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. Liu *et al.* proposed a 2ACK scheme in which the sending node waits for an ACK from the next hop of its neighbor to confirm that the neighbor has forwarded the data packet. However, this technique is vulnerable to collusions, i.e., the neighbor can forward the packet to a colluder which drops the packet.

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. Moreover, in routing protocols 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.

To mitigate routing misbehavior, existing works in mobile ad hoc networks reduce the traffic flowing to the misbehaving nodes by avoiding them in path selection. However, they cannot be directly applied to DTNs due to the lack of persistent path. 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. Li *et al.* proposed an approach that prevents the forgery of routing metrics. However, if the black hole node indeed has a good routing metric for many destinations, their approach will not work, but our approach still works by limiting the number of packets forwarded to the black hole node. Another related attack is the wormhole attack, which has been recently addressed by Ren *et al.*

III. PROPOSED SYSTEM

Proposed system consists of a packet dropping detection scheme and a routing misbehavior mitigation scheme. Fig. 1 illustrates our basic approach for misbehavior detection. The misbehaving node [N1 in Fig. 1] is required to generate a communication report during each contact and report its previous communication reports to the contacted node [N2 and N3 in Fig. 1]. Based on the reported communication reports, the contacted node detects if the misbehaving node has dropped packets. The misbehaving node may misreport (i.e., report forged communication reports) to hide its misbehavior, but forged records cause inconsistencies which make misreporting detectable.

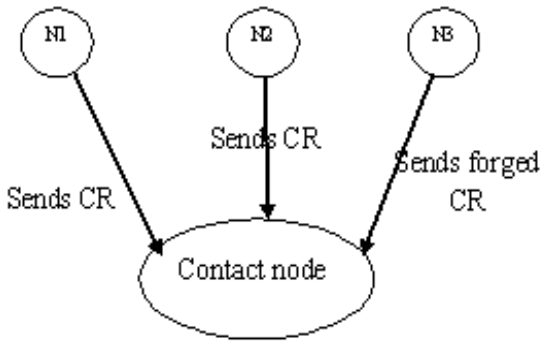

Fig. 1 Packet dropping detection misbehaving node reports forged communication report which is inconsistence.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

To detect misreporting, the contact node collects the communication report. It finds out which node has dropped the packets.

It reduces the data traffic that flows into misbehaving nodes in two ways: 1) If a misbehaving node misreports, it will be blacklisted and will not receive any packet from other nodes; 2) if it reports its communication reports honestly, its dropping behavior can be monitored by its contacted nodes, and it will receive much less packets from them.

3.1 BASIC IDEA

When two nodes contact, they generate a communication report which shows when this contact happens, which packets are in their buffers before data exchange, and what packets they send or receive during the data exchange. The record also includes the unique sequence number that each of them assigns for this contact. The record is signed by both nodes for integrity protection.

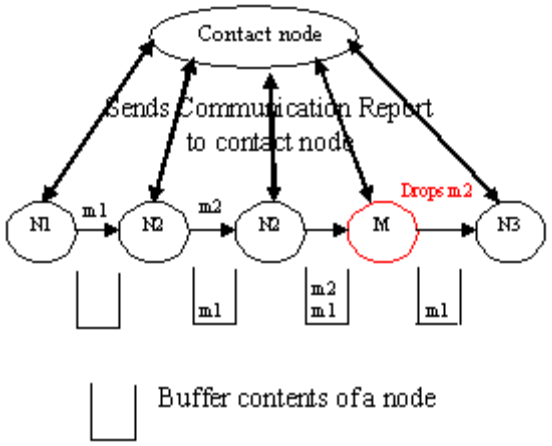

Fig 2. Examples of packet dropping detection and misreporting detection.

A misbehaving node may report a false record to hide the dropping from being detected. However, misreporting will result in inconsistent communication reports generated by the misbehaving node. To detect misreporting, for each communication report that a normal node generates with (or receives from) other nodes, the normal node selects witness nodes and transmits the record summary to them.

The summary only includes a part of the record necessary for detecting the inconsistency caused by misreporting. With some probability, the summaries of two inconsistent communication reports will reach a common witness node which will detect the misreporting node.

Consistency Rules: There exist two simple rules which are obeyed by normal nodes but violated by misreporting nodes:

- *Rule 1:* Use a unique sequence number in each contact.
- *Rule 2:* For two records signed by the same node, the record with a smaller contact time also has a smaller sequence number.

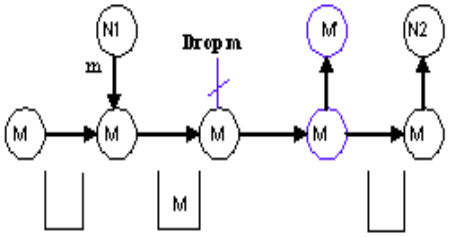

Fig 3. Two colluding nodes M and M' try to hide packet dropping of packet m by forging the communication report.

Suppose a misbehaving node drops a packet. If reports the true record of its previous contact to the next contacted (normal) node, the dropping can be detected. To hide the dropping, can forge a contact with its colluder after dropping the packet, and report the falsified communication report to the next contacted node, as illustrated in Fig. 3.

IV. SYSTEM ARCHITECTURE

The source sends data to the destination through the intermediate nodes. The intermediate node is acting selfish and misbehaves by dropping packets and it misreports it to the contact node. The contact node detects that node 3 has dropped packets and it sends the packet through node 4 to the destination. The contact node plays a vital role here in detecting the misbehaving node. Destination node on receiving the data sends the contact node an ack to intimate the receipt of data.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

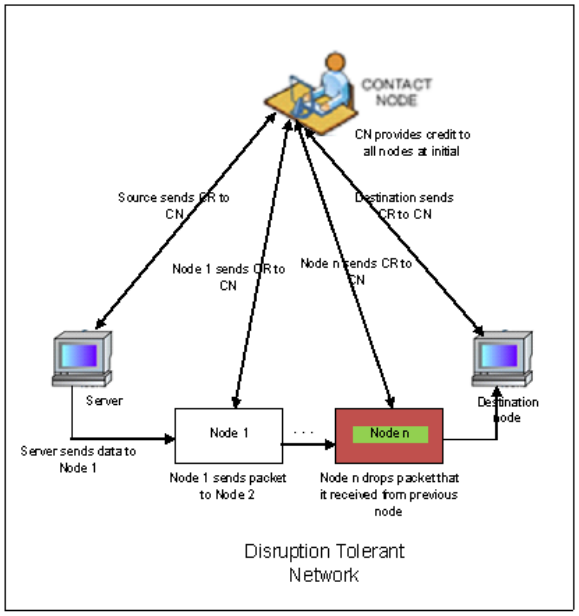

Fig: 4.1 (a) System architecture with misbehaving node

In Fig 4.1 (a) Node n misbehaves and drops packet that it receives from intermediate node. Node behaves selfish as it is unwilling to spend its resources to forward packets of other node. This reduces the packet delivery ratio and wasts system resources.

The source on receiving requests provides response to the client. Source forwards packet to node 1, which in turn forwards the packet to the next intermediate nodes, Source and intermediate nodes send CR to the contact node. This CR is used by the contact node to detect misbehaving nodes that drop packets. Node n misbehaves and it drops packet.

In Fig: 4.1(b) Node n which misbehaved is now renovated to legitimate node. The contact node detects it and renovates to legitimate node.

The contact node detects that node n has dropped packets using the CR. It provides credit to all nodes at the beginning. When a node misbehaves its credit value is decreased by CN. When a request is received from a client, its credit value is checked. If it's below a threshold value service to that client is rejected. In order to get service each node should maintain its credit value.

Thus misbehaving node behaves as legitimate node and forwards data to the destination or next intermediate nodes.

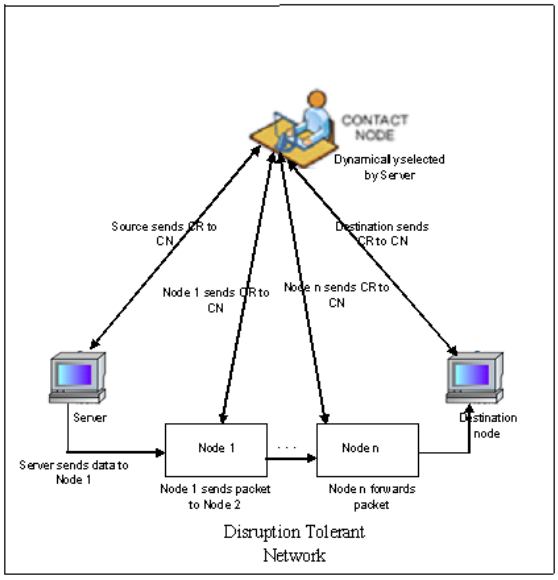

Fig: 4.1(b) System architecture with misbehaving node renovated to legitimate node

V. WORKING OF THE SYSTEM

In this scheme, a node is required to keep a few signed communication reports based on which the contact node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their communication reports to avoid being detected, the contact node applies the consistency rules. Source on receiving the request from receiver, serves it by transferring the required data. These data are transferred through a number of intermediate nodes. On each transfer between the nodes, the contact node receives the communication report. The communication report contains which shows when this contact happens, which packets are in their buffers before data exchange, and what packets they send or receive during the data exchange. The record also includes the unique sequence number that each of them assigns for this contact. The record is signed by both nodes for integrity protection.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)
International Conference on Information Systems and Computing (ICISC-2013), INDIA.

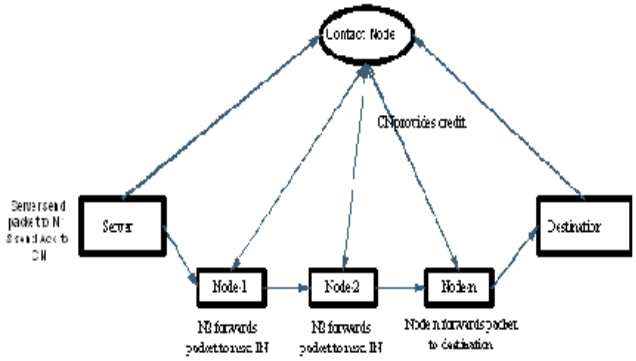

Fig. 5 Network resource identification

An interesting line of work attempts to packet forwarding schemes, where each node opportunistically forwards a packet to the neighboring node among multiple candidate nodes. The way to optimize the forwarding schemes for minimizing the expected packet delivery delays from the nodes to the Receiver or destination is studied this clearly reduces the delay. The data that are transmitted through the intermediate nodes are encrypted so that the data reaches the intermediate nodes in the encrypted form.

Misbehaving intermediate nodes drop the packets that are of no use to it and are unwilling to spend their resources for other nodes befits. Such misbehaving nodes are detected by the contact node using the communication report.

A distributed scheme is used to detect packet dropping in DTNs by the misbehaving nodes. As in Fig. 6 a node is required to keep previous signed communication reports such as the buffered packets and the packets sent or received, and report them to the contact node which can detect if the node has dropped packets based on the reported records.

To detect misreporting, the consistency rules are applied. The inconsistency is caused by the misreporting of misbehaving nodes. The consistency rules play a vital role in detection of misreporting.

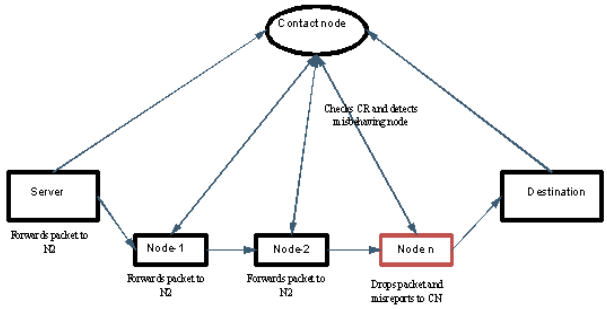

Fig. 6 Packet dropping

The contact node collects the communication reports that are generated when a node comes in contact with another during the forwarding of packets. When these contact nodes are static they have the chances of being compromised by the misbehaving nodes to avert it being detected. Hence the contact nodes are dynamically selected by the server during the commencement of packet transmission. The intermediate nodes that are not in the path of packet transmission are selected as contact nodes.

Misbehaving nodes drop packets that are of no use to them. These nodes are converted to legitimate node. A credit based scheme that can be used. Each node is given a same credit value by the contact node when a node enters the network. When a misbehaving node is detected its credit value is decreased. On receiving a request from client, server checks for its credit value. If the credit values are altered then it's a misbehaving node and service is denied for that client. To avail service from the server, the credit value should be maintained by each node. Thus misbehaving nodes will not prevail in network. The credit value is changed by contact node after a time period to make the misbehaving node a legitimate node. The data will reach the clients without any packet loss.

VI. Conclusion And Future Enhancement

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.

The further enhancement can be done by providing security to the contact node .This avoids the contact node being compromised by malicious node to avoid being detected.

Acknowledgements

I thank my project coordinator Mr. Muthukumarasamy M.E, my project guide Mr. C.Balakrishnan M.E (PhD), who are members of faculty with the Department of Computer Science and Engineering, S.A Engineering College, without whose guidance, this paper would not have been possible. I also wish to record my thanks to our Head of the Department Mrs.Umarani Srikanth M.E (PhD) for her consistent encouragement and ideas.

I would like to express my gratitude to all those who helped me make this paper a reality and gave me the opportunity to publish this paper.

REFERENCES

1. Journal Papers

[1] Nimitr Suanmali, Kamalrulnizam Abu Bakar and Suardinata "Selective Acknowledgement Scheme to Mitigate Routing Misbehavior in Mobile Ad Hoc Network" Vol. 8, Issue 3, No. 1, May 2011.

[2] Stephan Goebbels "Disruption tolerant networking by Smart Caching" International Journal of Communication Systems Volume 23, Issue 5, pages 569–595, May 2010.

[3] T.V.P.Sundararajan, Dr.A.Shanmugam "Selfish Avoidance Routing Protocol for Mobile Ad Hoc Networks" International Journal of Wireless and Mobile Networks, vol.2, May 2010.

[4] Suparna Biswas --- Sarmistha Neogy --- Priyanka Dey "Mobility Based Checkpointing And Trust Based Recovery In Manet "International Journal of Wireless & Mobile Networks Year: 2012 Vol: 4

2. Text Books

[1] Delay Tolerant Networks: Protocols and Applications edited by Athanasios V. Vasilakos, Yan Zhang, Thrasyvoulos Spyropoulos

[2] Delay- and disruption-tolerant networking: By Stephen Farrell, Vinny Cahill

3. Conference Proceedings

[1] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. ACM MobiCom, 000, pp.255–265.

[2] Buchegger and Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in Proc. MobiHoc, 2002, pp. 226–236.

[3] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting wormhole attacks in delay tolerant networks," IEEEWireless Commun.Mag., vol. 17, no. 5, pp. 36–42, Oct. 2010.

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

[6] B.-G. Chun, K. Chaudhuri, H. Wee, M. Barreno, C.H. Papadimitriou, and J. Kubiatowicz, "Selfish Caching in Distributed Systems: A Game-Theoretic Analysis," Proc. ACM Symp. Principles of Distributed Computing, pp. 21-30, 2004.

[7] D. Hales, "From Selfish Nodes to Cooperative Networks - Emergent Link-Based Incentives in Peer-to-Peer Networks," Proc. IEEE Int'l Conf. Peer-to-Peer Computing, pp. 151-158, 2004.

[8] N. Laoutaris, G. Smaragdakis, A. Bestavros, I. Matta, and I. Stavrakakis, "Distributed Selfish Caching," IEEE Trans. Parallel and Distributed Systems, vol. 18, no. 10, pp. 1361-1376, Oct. 2007.

[9] N. Laoutaris, O. Telelis, V. Zissimopoulos, and I. Stavrakakis, "Distributed Selfish RepLication," IEEE Trans. Parallel and Distributed Systems, vol. 17, no. 12, pp. 1401-1413, Dec. 2006.

[10] H. Miranda and L. Rodrigues, "Friends and Foes: Preventing Selfishness in Open Mobile Ad hoc Networks," Proc. IEEE Int'l Conf. Distributed Computing Systems Workshops, pp. 440-445, 2003.

[11] K. Paul and D. Westhoff, "Context Aware Detection of Selfish Nodes in DSR Based Ad-Hoc Networks," Proc. IEEE Global Telecomm. Conf., pp. 178-182, 2002.

[12] Y. Yoo and D.P. Agrawal, "Why Does It Pay to be Selfish in a MANET," IEEE Wireless Comm., vol. 13, no. 6, pp. 87-97, Dec. 2006.

[13] 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.

[14] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[15] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication

[16] attacks in sensor networks," in IEEE Symp. Security and Privacy, 2005, pp. 49–63.

[17] J. Zhai, Q. Li, and X. Li, "Data Caching in Selfish Manets," Proc. Int'l Conf. Computer Network and Mobile Computing, pp. 208-217, 2005.

[18] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc. IEEE INFOCOM, 2006, pp. 1–11.

4. Generic Website

[1] Disruption Tolerant Networking for Space Operations(DTN) http://www.nasa.gov/mission_pages/station/research/experiments/DTN.html(Accessed date: 13-Aug- 2012)

[2] Delay Tolerant Networking Research Group http://www.dtnrg.org/wiki/Docs(Accessed data: 2-sep-2012)

[3] Delay and Disruption Tolerant Network Security http://sprout.ics.uci.edu/projects/dtn/(Accessed date: 13-sep-2012)

[4] Towards Securing Disruption-Tolerant Networking http://research.nokia.com/files/tr/NRC-TR-2007-007.pdf