PERFORMANCE EVALUATION OF RAPID AND SPRAY-AND-WAIT DTN ROUTING PROTOCOLS UNDER BLACK HOLE ATTACK

Shally[1], Harminder Singh Bindra[2], Mamta Garg[3]

[1] *Student, CSE, BMSCE, Punjab, India*
[2] *Head of Department, IT, MIMIT, Punjab, India*
[3] *Assistant Professor, CSE, BMSCE, Punjab, India*

Abstract

DTN (Delay Tolerant Network) is a new concept in the field of wireless networks. It enables communication in challenged environment where traditional network fails. Unlike other ad hoc wireless network it does not demand for end to end node connectivity. DTN is based on store carry and forward principle. This mechanism is implemented using bundle protocol. DTN nodes have capabilities such as radio interface, movement, persistent storage, message routing and energy consumption .Here a node might accumulate a message in its buffer and carry it for limited time, waiting till a suitable forwarding opportunity is acquired. Multiple message duplication into the network is done to increase delivery probability. The main objective of DTN Routing is to build a powerful network between various nodes (mobile devices, planetary vehicles etc) so that good delivery probability and less delay are obtained. This unique mechanism poses a security challenge. A sophisticated attack observed is black hole attack in which malicious intermediate node are present in network that can provide attacked forged metrics to another node. The aim of this work is to simulate and analyze routing protocol of DTN when nodes enter in environment with black hole attack. The work has been carried out with ONE (opportunistic network environment) simulator. The performance of routing protocols (RAPID and Spray and Wait) are tested for different number of attacking nodes. The analysis indicates there is decrease in delivery probability, hop count average and buffer time average. But latency average first increases and then start decreasing. The overhead ratio increases using Spray and Wait Protocol but with RAPID protocol, it decreases with increasing black hole attacking nodes.

Index Terms: *DTN, ONE, etc.*

----------***----------

1. INTRODUCTION

In Existing heterogeneous wireless environment, node mobility, limited radio range, physical obstacles etc, wireless ad-hoc network helps to communicate between nodes without any existing infrastructure. Ad-hoc network algorithm assumes end to end connectivity between any pair of nodes that exists. Protocols like TCP/IP have a limitation over long distance. Because of long distance, high delay, low bandwidth, disruptive connections, harsh environment of space, satellite failures, solar flares, communications at deep space and non-habitat areas results into poor performance. Delay Tolerant Network is a way out for computer architecture that proved boon to the technical issues in heterogeneous network which may lack continuous connectivity [1].

DTN is based on the principle of store-carry-and-forward. This mechanism requires persistent storage and bundle protocols. Bundle is the basic unit of storage and transmission in DTN architecture. Bundle contains application data and is routed through intermediate nodes to final destination. In DTN node, bundle data passes through appropriate convergence layer then to transport protocol layer. Convergence layer of relaying nodes can be TCP, UDP etc. Transmission protocol provides essential protocol for transmission of bundle data to another DTN node. The store-carry and forward operates over multiple paths and extremely long timescales. Nodes act as a message ferries that carry messages between disconnected nodes [2]. It is advantageous as use of wireless bandwidth is not required but traffic flow need buffer space at message ferry. This unique mechanism poses a security challenge. DTN is vulnerable to confidentiality, integrity, authenticity, wormhole attacks etc. A sophisticated attack observed is black hole attack in which malicious intermediate nodes are present in network that can provide attacked forged metrics to another node. It also advertises itself as having the shortest path to the destination node [3].

In this Research paper, we have analyzed the performance of DTN routing protocol by implementing black hole attack on variable number of nodes.

2. APPLICATION OF DTN

DTN enabled network which is upgrading interplanetary communication. DTN network has less risk, increased

robustness, low human labor cost, maximum link utilization efficiency. It has applications [5] such as

1) Space application: Internet for planets gets a very good option with this DTN technology. DTN idea has enhanced International Collaboration by exploring space. Consultative Committee for Space Data Systems has been working to standardize space communications around DTN as shown in fig. 1. US astronaut Sunita Williams took control of the ESA (European space agency) DTN Lego rover (Robot) while orbiting high in the sky aboard the International Space Station in the year 2012 [4].

2) Earth application: File transfer, web browsing and exchanging emails can be done at better speed with DTN implementation as in sensor network, military applications, mobile devices etc.

3) Underwater application: Exploring, monitoring sea bed area where exploring get simple and fast with DTN.

4) Non-Habitant area application: The fast network communication can be facilitated in non-habitat area.

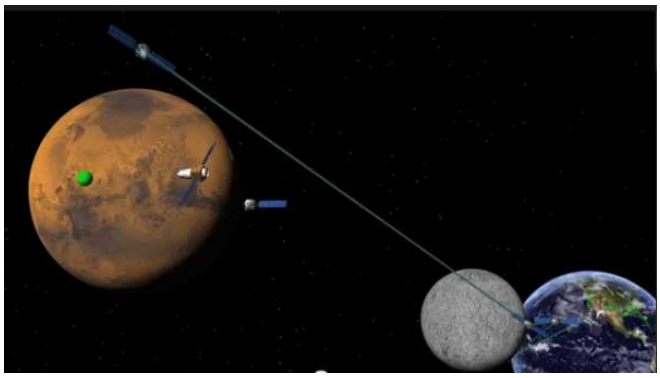

Fig -1: Space communications around DTN

3. ROUTING PROTOCOLS IN DTN

Routing provides a solution on the existence of wireless network. Links between nodes are not persistent in time, sparse and network topology which changes frequently. DTN routing schemes aims to route message packet into network so as to have minimum utilization of resources, maximum delivery probability and less delay. Various types of protocols can be classified

a) Epidemic protocol: In Epidemic protocol [6] simply replicates messages to all encountered nodes but stops if predefined hop count's maximum value is reached. Messages are not send to encountered node if a copy of message is already present with this node. Overhead gets high due to more utilization of buffer space but delivery probability gives good value.

b) Spray and Wait protocol: Spray and Wait protocol is n-copy routing protocol. This routing algorithm consists of two phases: spray followed by wait. Here, number of copies to be created is beforehand decided. Suppose n copies are sprayed to relay in network, then they enter the wait phase until they meet the destination and message is finally delivered. Two Spray and Wait models are suggested by authors:

- Normal mode: In this case, sender node replicates a message to all nodes that are encountered. Only n nodes get copy because there are n message copies available.
- Binary mode: In this case, out of n copies, n/2 copies are stored by sender node and remaining copies to all first encountered nodes. These n/2 stored copies are then relayed until a single copy is left and last copy is forwarded to final destination [7].

c) PRoPHET protocols: PRoPHET Protocols is predictive protocol which studies the encountered node to make routing decisions. Overhead will be less because of this predicting nature. It calculates node probability for specific destination [8]. If a given message in encountered node E has high delivery predictability then sender node transmit a copy to this E node. Delivery predictability of intermediate node can be decided on the basis of

- Number of encounters of E.
- Time lasting for these encounters and
- Existence of these transitive properties for mutual encounters of this node.

d) MaxProp protocol: In MaxProp protocol maximum probability of message to be delivered is calculated. Packets in buffer are prioritized. Lower the hop count value, higher is the probability set and if hop count value exceeds the threshold value then priority of packet is determined by calculating the probability of nodes meeting [9].

e) RAPID protocol: RAPID models DTN routing as a utility-driven resource allocation problem. A packet is routed by replicating it until a copy reaches the destination. It derives a per-packet utility function from the routing metric. At a transfer opportunity, it replicates a packet that locally results in the highest increase in utility. In general, Ui is defined as the expected contribution of I to the given routing metric. For example, the metric minimize average delay is measured by summing the delay of packets. Accordingly, the utility of a packet is its expected delay. Thus, rapid is a heuristic based on locally optimizing marginal utility, i.e., the expected increase in utility per unit resource used. Rapid replicates packets in decreasing order of their marginal utility at each transfer opportunity. Protocol rapid(*X*, *Y*):

- Initialization: Obtain metadata from *Y* about packets in its buffer and metadata *Y* collected over past meetings.

- Direct delivery: Deliver packets destined to *Y* in decreasing order of their utility.
- Replication: For each packet i in node *X*'s buffer
  i. If *i* is already in *Y*'s buffer (as determined from the metadata), ignore *i*.
  ii. Estimate marginal utility, ∂Ui, of replicating *i* to *Y*.
  iii. Replicate packets in decreasing order of $\partial Ui / Si\neg$.
- Termination: End transfer when out of radio range or all packets replicated [10].

In this study we have taken RAPID and Spray and Wait protocols for analysis.

4. METHODOLOGY

In this section the working principle of simulation tools used, scenarios used are being described for analysis, simulation setup, metrics and comparisons using graphs.

4.1 Simulation tool used

The work is performed by the use of ONE (Opportunistic Network Environment) simulation tool [11]. It is simulating environment to facilitate users to rapidly generate realistic mobility network for DTN Simulation. This single simulation framework is Java based tool. Features of ONE simulator are

- Modular fashion builds software.
- Node movement modeling
- Internodes contact
- Message handling
- GUI display the complete scenario
- Reports summarize the complete simulation.
- Routing information of particular field(message) can be referred

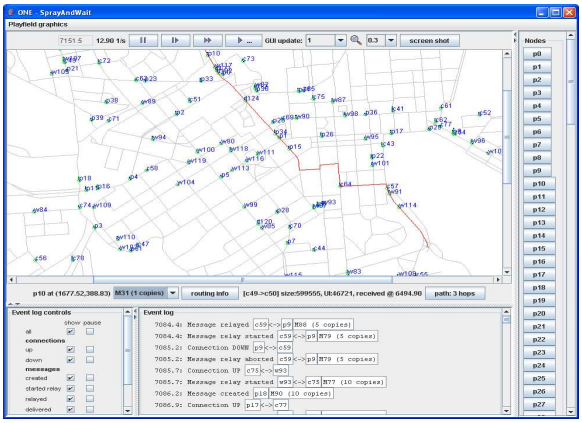

Fig -2: Screenshot of ONE Simulation

It creates a GUI main window as shown in fig 2.It is divided into three parts

- Top section: Buttons are present on top to pause, step, fast forward the simulation. Zoom option and GUI speed can also be adjusted.
- Main part: It shows complete simulation over map where paths are defined and node identifiers specify nodes. The communication among nodes and messages transfer between different nodes can also be visualized.
- Right part: For closer inspection of node, its messages, routing information can be checked by clicking on button identifying a particular node's name using their group id.

Results can be checked through visualization, reports and post processing tools. For this experiment two reports are specifically used: Event Log Report and Message Status Report.

4.2 Simulation Setup

Simulating environment consists of total 50 hosts belonging to single group. Simulation is checked with 5 black hole attacking nodes proceeding with 10, 15, 20 till 50 i.e. total numbers of nodes in complete scenario. The table list the details of simulation setup, over this scenario, number of nodes are made to attack as Black hole attack.

Table 1: Simulation parameters

PARAMETER	VALUE
Total Scenario time	43200 sec
Routing Protocol	RAPID; Spray and wait
Movement Model	ShortestPathMapBased Movement
Interface Transmit Speed of message	560 kbps
Interface Transmit Range	30 m
Message total time to live	90 min
Nodes Buffer Size	25M
Total number of Host	50
Node movement speed	Min=1.9m/sec Max=3.9m/sec
Message creation interval	One message per 15 – 30 sec
Message size	250KB to 2MB

4.3 Simulation parameters

For this study five performance metrics are selected namely [12]:-

1. Delivery Probability: Delivery probability defines the probability of message being delivered to final destination successfully.
2. Latency Average: It is average of message delay from creation to final delivery at destination.
3. Hop count average: It is average of number of hops between source and destination nodes.
4. Buffer time average: It is average of time for which message stayed in buffer at each node.
   Buffer time average = [Creation / Received][Next Hop].
5. Overhead Ratio: It access to the bandwidth efficiency.

i.e.
(Number of Relayed Messages – Number of Delivered Messages) / Number of Delivered Messages

- Round trip time average: It is average time from creation to the confirmation delivery. But for the all scenarios it gives NAN i.e. Not any number because protocol does not support response

5. RESULTS AND ANALYSIS

The DTN routing protocol is being simulated over a realistic mobility model and the results are analyzed under different number of black hole attacks.

A. Delivery Probability vs. Number of Malicious nodes

In this case, successful delivery probability is analyzed with varying number of malicious number of nodes as shown in fig. 3.

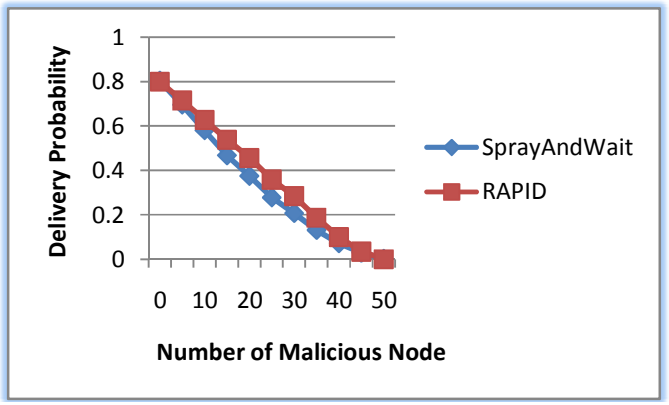

Fig -3: Delivery Probability vs. number of malicious nodes

Inference: Delivery Probability decreases constantly with the increase in number of malicious nodes. As the number of malicious nodes are increasing i.e. nodes dropping messages from their buffer spaces are increasing in number and resulting in loss of message copies from node's buffer space. It further results in decrease in delivery of message at destination. Delivery probability is more for RAPID protocol than Spray and Wait protocol. At the end delivery probability reaches zero as no message is delivered when all nodes are malicious.

B. Latency Average vs. Number of Malicious nodes

In this case average message delay variation is observed by varying number of malicious as shown in the fig. 4.

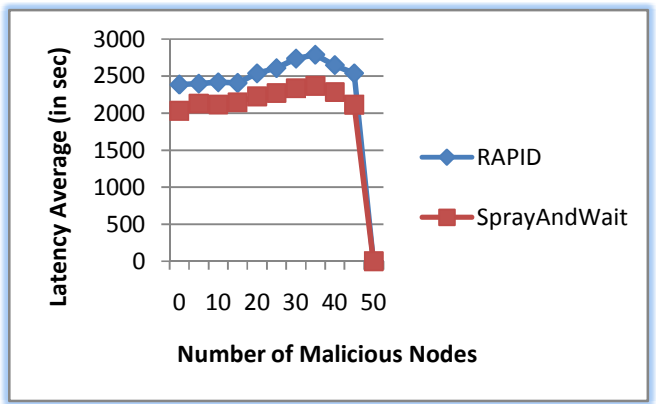

Fig -4: Latency average vs. number of malicious nodes

Inference: Latency average is increasing but at the end when more than 90% nodes are malicious then it decreases. As delivery probability is decreasing and messages that are delivered in the presence of malicious nodes are those that are delivered by non-malicious nodes and they are decreasing continuously so latency average ultimately increases. For RAPID, latency average is more than Spray and Wait protocol. The decrease at the end is because messages that are delivered are those whose destination lies near and destined messages at far of are delayed or dropped as malicious nodes are increasing. At the end value is zero because delivery probability is almost zero at end.

C. Hop count average vs. Number of Malicious nodes

In this case, hop count average is analyzed with varying number of malicious number of nodes as shown in the fig. 5.

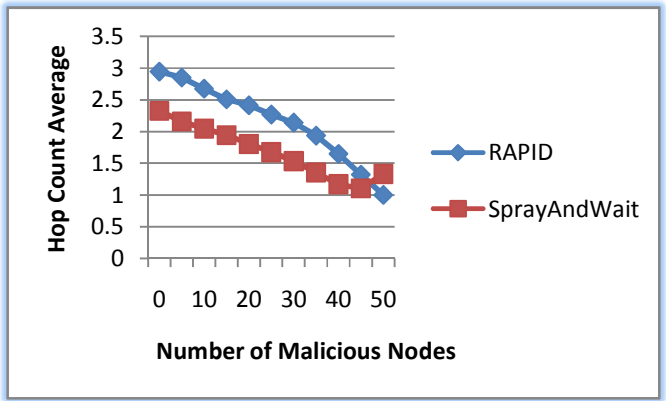

Fig -5: Hop count average vs. number of malicious nodes

Inference: Hop count average decreases constantly at the cost of delivery probability with the increase in number of malicious nodes. As malicious nodes are increasing, delivery probability is decreasing and delivered message in this scenario are those that results in from the process of less number of hop counts. Hop count average is more for RAPID protocol than Spray and Wait protocol. At the end, hop count is not equal to zero.

D. Buffer time average vs. Number of Malicious nodes

In this case, buffer time average is analyzed with varying number malicious nodes as shown in fig. 6.

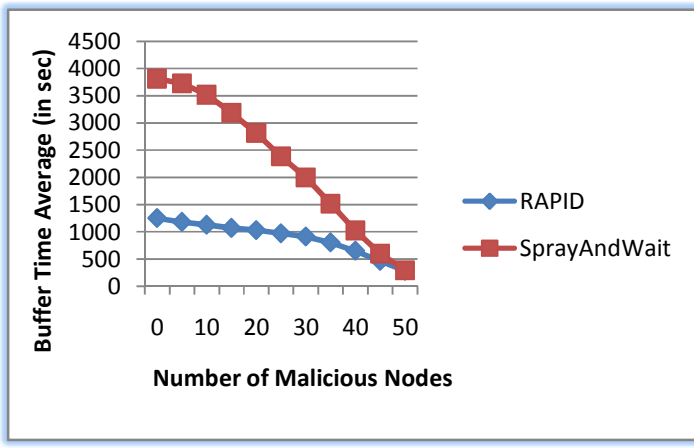

Fig -6: Buffer time average vs. number of malicious nodes.

Inference: Buffer time average decreases constantly with the increase in number of malicious nodes. As malicious nodes are dropping messages from their buffer space which further affect the process of store-carry-forward in encountered nodes. So time for which message stays in buffer space decreases with increase in malicious nodes. Buffer time average is more for Spray and Wait protocol than RAPID protocol because spray and wait protocol create n replicas unlike RAPID protocol which creates replicas upon utility check of packet.

E. Overhead ratio vs. Number of Malicious nodes

In this case, overhead ratio is analyzed with varying number malicious nodes.

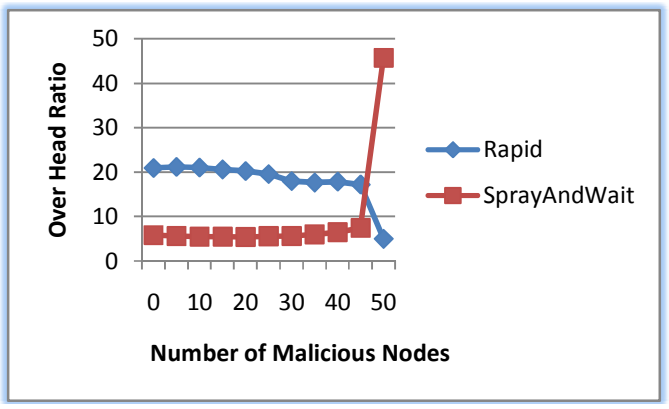

Fig -7: Overhead ratio vs. number of malicious nodes

Inference: Overhead increases with the increase in number of malicious nodes using Spray and wait protocol but with RAPID, it decreases with increasing number of malicious nodes. RAPID protocol maintain routing metrics, as it evaluates per packet utility, so data structures , data values are to be stored and results into high overhead. It is decreasing for RAPID protocol because malicious nodes are increasing and many messages are dropped. The utility function calculations for message are decreasing with dropping of messages. At the end no message is left for per packet utility check because almost all nodes are malicious and maximum messages are dropped. Spray and wait protocol do not follow any calculated path but choose randomly encountered node to forward the replicas so overhead is less. At the end, delivery probability is almost zero so as per the formula of overhead ratio, overhead is increasing

CONCLUSION

DTN are important research field which is emerging nowadays. It works with normal working of objects, human, animals, vehicle, planets etc. It defines the important technology required in interplanetary system, deep space communication. With Delay Tolerant Network monitoring gets very easy, internet can be facilitated with very good speed etc. DTN is simulated using ONE simulator. It is java based tool. The experiment has been performed with varying number of black hole attacking nodes. The simulation is analyzed and two protocols (i.e. RAPID and Spray and Wait) are compared on the basis of performance parameters i.e. delivery probability, overhead ratio, buffer time average, latency average and hop count average. They are affected by varying malicious nodes. Following observations are made

- Delivery probability decreases with the increase of number of attacking nodes. It is more for Spray and Wait protocol initially but when malicious nodes are present then RAPID protocol has higher value than Spray and Wait protocol.
- Overhead ratio is more for RAPID than Spray and Wait. Overhead ratio increases for spray and wait but for RAPID protocol decreases with the increase of number of attacking nodes.
- Latency average increases with increasing number of nodes and at end latency average suddenly decreases. It is more for RAPID than Spray and Wait protocol.
- Buffer time average decreases with increases in number of attacking nodes. It is more for Spray and Wait than RAPID protocol.
- Hop count average is continuously decreasing with increasing number of attacking node. It is more for RAPID protocol than Spray and Wait protocol.
- The analysis clearly shows that RAPID protocol gives best result for delivery probability and buffer time average. Spray and Wait protocol gives good result for overhead ratio, latency average and hop count average.

In future we would like to explore the performance of other routing protocols in more adverse cases and these protocols in more adverse cases.

ACKNOWLEDGEMENTS

I would like to thank all anonymous reviews for their constructive feedback on the work presented over here

REFERENCES:

[1]. S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott and H. Weiss, "Delay-tolerant networking: an approach to interplanetary internet," IEEE Communications Magazine, vol. 41, 2003, pp. 128-136.

[2] K. Scott, S. Burleigh, "Bundle Protocol Specification".RFC 5050, November 2007.

[3]Contemporary survey of DTN Security [Online].Available:http://web.nmsu.edu/~chssrk/conclusions.shtml last accessed on 28th December 2013.

[4]NASA Website [Online].Available at http://www.nasa.gov/home/hqnews/2012/nov/HQ_12-391_DTN.html last accessed on 28th December, 2013.

[5] K. Fall, "A delay-tolerant network architecture for challenged internets," SIGCOMM Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications, pp. 27-34, ISBN: 1-58113-735-4

[6] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Technical Report CS-200006, Duke University,April 2000.

[7] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "spray and wait: an efficient routing scheme for intermittently connected mobile networks," in Proc. of the ACM SIGCOMM Workshop on Delay- Tolerant Networking (WDTN), 2005.

[8] A. Lindgren, A. Doria, and O. Schelen, "Probabilistic routing in intermittently connected networks," in The First International Workshop on Service Assurance with Partial and Intermittent Resources (SAPIR), 2004.

[9]. J. Burgess,B.Gallagher, D. Jensen and B.N. Levine, "MaxProp: Routing for vehicle-Based Disruption-Tolerant Networks," Proceedings of 25th IEEE international Conference on Computer Communications, Barcelona, 23-29 April 2006, pp. 1-11.doi:10.1109/INFOCOM.2006.228.

[10]. B. Aruna, L. B. Neil, and V. Arun, "DTN Routing as a Resource Allocation Problem," SIGCOMM'07, Kyoto, Japan, August 27–31, 2007.

[11]. A. Ker¨Anen, "Opportunistic network environment simulator. Special assignment report, helsinki university of technology," Department of Communications and Networking, May 2008.

[12]. H.S. Bindra and A.L. Sangal, "Performance comparison of RAPID, Epidemic and Prophet Routing Protocols for Delay Tolerant Networks," International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012.