IMPLEMENTATION AND ANALYSIS OF IDENTITY SPOOFING ATTACK USING EPIDEMIC ROUTING PROTOCOL IN DTN

[1]Saroj Rani, [2]Er. Abhilasha, [3]Er.Swati Jindal
[1]M.Tech (Student), [2]Associate Professor, [3]Assistant Professor
GZS Campus
Email:[1]ashgoyal629@gmail.com, [2]abd_jain@rediffmail.com, [3]er.swati.jindal87@gmail.com

Abstract:-Now these days Delay Tolerant network (DTN) is used rather than ad-hoc networks because if no end-to-end path between the nodes then DTN work in that situation including emergency scenarios and battlefield applications. In DTN is to maximize probability of delivered messages is the main objective. In this protocols Epidemic, Spray-and-Wait (SNW) and Prophet are compared and analyzed using one simulator and then identity spoofing attack in epidemic routing protocol has been applied and the effect of this attack on working of routing protocol for delivery probability, overhead ratio, buffer time and latency has been analyzed.

***Keywords:* - Delay Tolerant Network (DTN), Epidemic Routing Protocol, Identity Spoofing Attack.**

I. INTRODUCTION

Today’s Internet has been successful at connecting devices through which communicate around the world. In this using various set of protocols which has been made i.e. known as TCP/IP protocol for transferring data from source to destination with the minimum delay and high reliability. End-to-End transfer of data and connectivity is the main principle of TCP/IP protocol. If there is no path between source to destination at any time then this protocol not work and whole system stops working completely. Then new network developed i.e. DTN (Delay Tolerant Network) in which there is no end to end connectivity [2] [14] [16] shown in figure 1.1. There are various “challenged” areas i.e. deep space networks, outer-space networks, under-water networks, sensor networks, vehicular networks, mobile ad-hoc networks, military networks, exotic media networks, inter-planetary networks [1][8][14][15] through which communicate. Lack of Connectivity, Irregular Delays, High Latency ,Low data rate, Short Range Contact are characteristics of Delay Tolerant Networks [1][23].

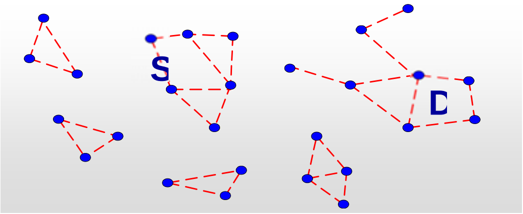

Figure 1.1- Delay Tolerant Network [17]

A. *Architecture of Delay Tolerant Network*

The architecture of DTN contain various assumptions and conditions of the TCP/IP Protocol based networks and includes the concept of regions and gateways.DTN architecture shown in figure 1.2 is based on the following parts or principles [2] [14].

- Region is part which is similar to network stack and addressing
- DTN gateways are interconnected points between no similar network protocol and addressing families called regions e.g. Internet-like, Ad-hoc, Mobile etc performs reliable message routing and security checks

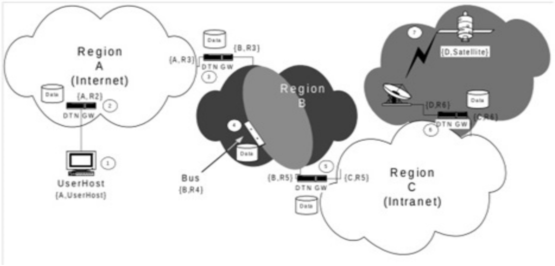

Figure 1.2 –Delay Tolerant Network Architecture [11]

B. Routing in DTN

In Delay Tolerant Network, measure the cost of delivering messages from one place to another a distance function is used in it. It requires only small information about the network to route the messages and routing is the main challenge in DTN. The connectivity of DTN is difficult to ensure end-to-end delivery of data and delays makes it impossible to provide acknowledgements and retransmissions. The objectives of routing, is to maximize the probability of delivered messages. Routing in DTN mainly includes two types i.e. flooding and forwarding strategies include protocols shown in Table 1.

Table 1-Routing Protocols in DTN

Flooding Strategies	Forwarding Strategies
Epidemic Protocol	PROPHET
RAPID	FRESH
Spray And Wait	MAXPROP
Prioritized Epidemic	MV(MEET ND VISIT)
FUZZY SPRAY	
Spray And Focus	

C. Routing Techniques in DTN

Store Forward Technique: - The problems are covered in DTN that are associated with protocols in terms of lack of connectivity, irregular delays and asymmetric bidirectional data rates etc. use store and forward technique. In this node store the message until communication arises in it. Figure 1.3 use method of store and forward i.e. analogous to real life postal service.

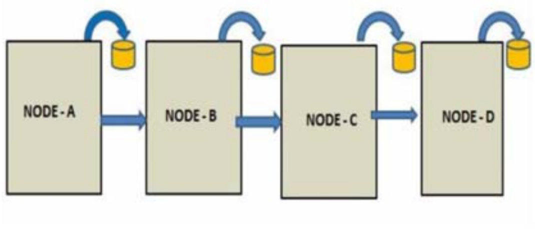

Figure 1.3 - Store and Forward Approach [14]

Custody Transfer Technique: - In this delivered the message from one DTN hop to the next and passing of reliability delivery responsibility. DTNs support error-checking of transferred messages. If data lost or corrupted then retransmission of messages is done. In case of no acknowledgement, retransmission of the message occurs. Two types of nodes that can be persistent and non-persistent. In persistent nodes assumed to contain persistent memory storage and participate in custody transfer. A non-persistent node transfer custody of a message to a persistent node which accepts responsibility for reliably delivering the message.

D. Routing Strategies

The connectivity of DTN makes difficult to ensure end-to-end delivery of data. Routing in Delay Tolerant Networks can be classified into 2 types. These are as:-

- Flooding Based.
- Forwarding Based.

Flooding Based: - In Flooding based routing in DTN, each node has a number of copies and transmits them to set of nodes and these are called relays. In this all relays maintain the copies in buffer space until they connect with another node. In this no knowledge about the network. Flooding network with messages will consume network resources like bandwidth, buffer, node energy etc.

Forwarding Based: **-** This is also called history based approach because histories of encounters are exploited in many works and research areas. Zebranet project is one of major to use history of encounters for routing decisions and use to delivery of messages. In this no use of replication in it and use best path to send the message. In this approach protocols are used in it i.e. Probabilistic Routing Protocol using History of Encounters and Transitivity (PROPHET), Fresher Encounter Search (FRESH), MaxProp etc.

E. *Related Work*

Vahdat and Becker et al. (2000) [18] proposed Epidemic routing protocol i.e. flooding based forwarding algorithm and spread message in Omni direction. Lindgren et al. (2003) [19] developed the probabilistic routing protocol using history of encounter and transitivity (PROPHET) that has more delivery probability. Spyropoulos et al., (2005) [20] developed the spray and wait routing protocol to control level of messages that are spread throughout the network. John Burgess et al. (2006) [21] proposed MaxProp, a protocol for routing of DTN messages. Aruna Balasubramanian et al.(2007) [22] RAPID, an intentional DTN routing protocol that can optimize specific routing metric such as worst-case delivery delay or fraction of packets that are delivered within a deadline shown in table

Table 2- DTN Routing Protocols

Name of the Protocol	Year	Work Done
EPIDEMIC ROUTING PROTOCOL	2000	NO KNOWLEDGE ABOUT THE NETWORK. LARGE NUMBERS OF MESSAGES ARE TRANSFERRED AND MULTICOPY SCHEME USED IN IT.
PROPHET	2003	HISTORY BASED AND USING DELIVERY PREDICTABILITY TO DELIVER A MESSAGE FROM ONE TO ANOTHER NODE.
SPRAY AND WAIT PROTOCOL	2005	IN THESE TWO PHASES ARE USED IF FIRST NOT DELIVERED MESSAGE AT DESTINATION THEN WAIT PHASE DIRECTLY DELIVER THE MESSAGE FROM NODES. REDUCE OVERHEAD AND CONGESTION.

F. *Attacks in DTN*

A spoofing attack is when any fake node party represents another device or user on a network in order to develop attacks against network hosts, steal data or bypasses access controls. There are several different types of spoofing attacks that faked parties can use to accomplish this. In this generally have four general attacks i.e. Drop All, Random flooding, Invert routing metadata and Acknowledgement counterfeiting were shown to be ineffective. Although the above attacks may be ineffective, many variant of attacks are still possible. Various attacks in it are blind spoofing attack, non-blind spoofing attack and Denial-of-service attack.

In blind spoofing attack cracker transmits the packets to target in sequence number and then falsify his identity by injecting data into stream of packets without authenticated him.

In non blind spoofing attack if sequence is known attacker can hijack session that has already built and bypass authentication that was conducted on previous connection.

In Denial-of-Service attack multiple hosts send the packets to DOS .in that case transmission is spoofed and difficult to track down the sources of storm.

G. *Security in Delay Tolerant Network*

In DTN various resources indicate that some form of authentication and control the network in various ways. It is not possible for the unauthorized user to use the network in easy way and it is possible for only authorized users. In some cases it is not possible for unauthorized user to be forwarded to certain network links using Table 3 to describe easily.

Shally et al. (2014) [23] under the black hole attack to analyze the performance of RAPID and SPRAY-and-WAIT DTN routing protocols. Preeti Nagrath et al. (2014) [24] perform flooding attack in delay tolerant networks. Harminder Singh Bindra et al. (2014) [25] using Routing Attack to investigate the Performance of Extended Epidemic Routing Protocol of DTN. Yinghui Guo et al., (2013) [26] in Vehicular Delay Tolerant Networks detect the Blackhole and Greyhole Attacks. Yanzhi Ren et al. (2010) [27] analyze wormhole attacks in delay tolerant networks. Fai Cheong Choo et al. (2010) [28] detect Robustness of DTN against Routing Attacks.

Table 3-Various Security Mechanisms in DTN

Year	Name of Paper	Protocol/mechanism	Attack
2014	PERFORMANCE EVALUATION OF RAPID AND SPRAY-AND-WAIT DTN ROUTING PROTOCOLS UNDER BLACKHOLE ATTACK	RAPID AND SPRAY-AND-WAIT	BLACK HOLE ATTACK
2014	FLOODING ATTACK IN DELAY TOLERANT NETWORK	EPIDEMIC,PROPHET,MAXPROP, SPRAY-AND-WAIT	FLOODING ATTACK
2014	INVESTIGATIG PERFORMANCE OF EXTENDED EPIDEMIC ROUTING PROTOCOL OF DTN UNDER ROUTING ATTACK	EPIDEMIC	ROUTING ATTACK
2013	DETECTING BLACKHOLE AND GREYHOLE ATTACKS IN VEHICULAR DELAY TOLERANT NETWORKS	EPIDEMIC AND SPRAY-AND-WAIT	BLACKHOLE GREYHOLE ATTACKS
2010	DETECTING WORMHOLE ATTACKS IN DELAY-TOLERANT NETWORKS	PROPHET	WORMHOLE ATTACK
2010	ROBUSTNESS OF DTN AGAINST ROUTING ATTACK	MAXPROP	ROUTING AT

II. SIMULATION AND RESULT ANALYSIS

Simulation Environment:-To set up the simulation using **one simulator**. In our simulation we have assigned simple broadcast type Bluetooth interface to compare to real time application and used to better judge the performance of Epidemic routing protocol. The complete simulation setup information is given in Table 4. Delivery Probability and Overhead Ratio performance metrics are considered for the research work and show the work using parameters.

(i) *Delivery Probability*: Fraction of developed messages that are correctly delivered to the destination within given time period.

(ii) *Overhead Ratio:-R*atio between the total transmissions over the number of delivered messages.

Table 4-Simulation Setup Information

Parameters	Value
Simulation Time	43200.1000
Interface	Blue tooth Interface
Routing Protocols	Epidemic,SNW,Prophet
Buffer size	50 messages
No. of nodes	50
Msg TTL	300(5 hours)

A. *Analysis and comparison of Epidemic, SNW, Prophet protocols*

Delivery Probability: - Figure 1.4 shows the comparison between the three protocols i.e. Epidemic, Spray and wait and PROPHET. Delivery probability of SNW has 38.74% as compared to others.

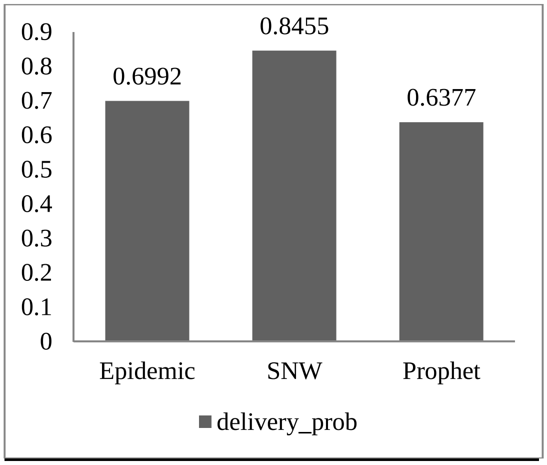

Figure 1.4 -Comparison Chart of delivery probability of Epidemic, SNW and Prophet

Overhead Ratio: - Figure 1.5 compares overhead ratio of all three protocols .Prophet protocol has overhead ratio i.e. 47.39%.

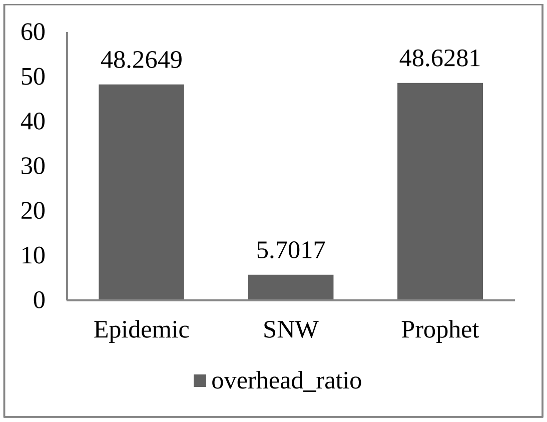

Figure 1.5 -Comparison Chart of Overhead Ratio of Epidemic, SNW and Prophet.

B. Implementation and Analysis of Identity spoofing attack on one node

Implement and analyze the attack on one node using same simulation environment shown in Table 4 but using only Epidemic Routing Protocol.Figure 1.6 show effect of attack on one node shows 4 fake delivered message and without attack shows 1023 messages that are delivered.Fakedelivered messages means messages of real node goes to fake node.

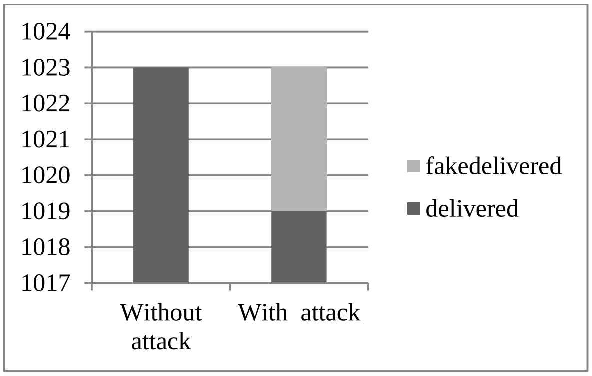

Figure 1.6–Comparison of effect of attack on one node

C. Implementation and Analysis of Identity spoofing attack on multiple nodes.

Delivery Probability:-If identity spoofing attack applied on the nodes then delivery probability has 49.9% and if attack not applied on it then its 50.1%.

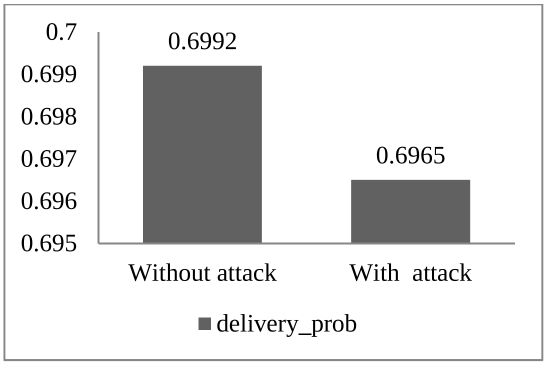

Figure 1.7 –Comparison of effect of attack on multiple node

Overhead Ratio: - If identity spoofing attack applied on the nodes then overhead ratio has 50.1% and if attack not applied on it then its 49.9 %.

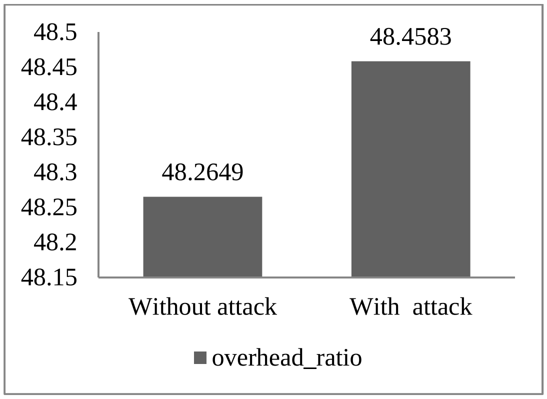

Figure 1.8 –Comparison of effect of attack on multiple nodes

III. CONCLUSION

Delay Tolerant Networks will form most important facts of modern day networking given the connectivity. The traditional TCP/IP protocol suite is not suited when there is no end to end connectivity in the networks. In DTN have many applications that have capabilities that can extend to applicable to challenged networks such as used by space, military and intelligence areas. In this there are various protocols that are using various parameters and perform operation on this using one simulator and apply attack on epidemic in delay tolerant network. It also checks the performance, bandwidth, latency of the different-different protocols and also checks which is higher and which is lower in it.

REFERENCES

[1] Kevin Fall "A Delay-Tolerant Network Architecture for Challenged Internets" IRB-TR-03-003 February, 2003

[2] Kevin Fall "A Delay-Tolerant Network Architecture for Challenged Internets" SIGCOMM'03, Karlsruhe, Germany August 25-29, 2003.

[3] Kevin Fall (kfall@intel-research.net) "A Delay-Tolerant Network Architecture for Challenged Internets" SIGCOMM'03 Intel Research, Berkeley Presented by Sookhyun, Yang Nov. 26, 2003

[4] Ari Ker anen "Opportunistic Network Environment simulator" May 29, 2008

[5] Ari Keränen, Jörg Ott and Teemu Kärkkäinen "The ONE Simulator for DTN Protocol Evaluation", SIMUTools 2009, Rome, Italy.

[6] R. J. D'Souza and Johny Jose "Routing Approaches in Delay Tolerant Networks: A Survey"International Journal of Computer Applications (0975 - 8887)Volume 1 – No. 17 ©2010

[7] Harminder Singh Bindra and Amrit Lal Sangal "Considerations and Open Issues in Delay Tolerant Network's (DTNs) Security" Wireless Sensor Network, 2, 645-648,2010

[8] Morteza karimzadeh "Efficient Routing Protocol in Delay Tolerant Network "may 2011

[9] Abey Abraham and Jebapriya S "Routing strategies in Delay Tolerant Networks: a Survey" International Journal of Computer Applications (0975 – 8887) Volume 42– No.19, March 2012

[10] Khalil Massri, Alessandro Vernata and Andrea Vitaletti PM2HW2N'1 "Routing Protocols for Delay Tolerant Networks: a Quantitative Evaluation" 2, Paphos, Cyprus, October 21–22, 2012.

[11] Kevin Fall Presented by Ross Lagerwall "A Delay-Tolerant Network Architecture for Challenged Internets" March 5, 2013

[12] Chintan B. Desai Mr. Vyomal N. Pandya and Dr. Prashant M. Dolia Chintan B. Desai et al./ "Comparative Analysis of Different Routing Protocols in Delay Tolerant Networks" International Journal of Computer Science & Engineering Technology (IJCSET) ISSN : 2229-3345 Vol. 4 No. 03 Mar 2013

[13] Mamoun Hussein "Efficient DTN Routing Protocol" International Journal of Computer Applications (0975 – 8887) Volume 80 – No.9, October 2013

[14] SuvarnaPatil*,Geetha R. Chillerge** Suvarna Patil et al "Delay Tolerant Networks – Survey Paper" Int. Journal of Engineering Research and Applications www.ijera.com ISSN : 2248-9622, Vol. 4, Issue 2(Version 2), February 2014, pp.21-25

[15] Kevin Fall "A Delay-Tolerant Network Architecture for Challenged Internets" Anshul Kantawala November 23, 2015

[16] Md. Raiyan Alam and Bibekanand Minz"Routing in Delay Tolerant Networks"

[17] Jim Kurose and Keith Ross "Routing-DTN"

[18] Amin Vahdat and David Becker(2000) "Epidemic Routing for Partially-Connected Ad Hoc Networks "

[19] "Prophet routing poster" Lindgren *et al.*13 April 2011

[20] Thrasyvoulos Spyropoulos, Konstantinos Psounis, CauligiS. Raghavendra "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks" SIGCOMM-2005, Philadelphia

[21] John Burgess Brian Gallagher David Jensen Brian Neil Levine "MaxProp : Routing for Vehicle-Based Disruption-Tolerant Networks"

[22] Aruna Balasubramanian, Brian Neil Levine and Arun Venkataramani "DTN Routing as a Resource Allocation Problem" SIGCOMM'07, Kyoto, Japan, August 27–31, 2007.

[23] Shally1, Harminder Singh Bindra2, Mamta Garg3 "PERFORMANCE EVALUATION OF RAPID AND SPRAY-AND-WAIT DTN ROUTING PROTOCOLS UNDER BLACK HOLE ATTACK" IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308 Volume: 03 Issue: 01 | Jan-2014, Available @ http://www.ijret.org

[24] Preeti Nagrath1, Dr. Sandhya Aneja2, Prof. G. N. Purohit3 "Flooding Attack in Delay Tolerant Network" International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)

[25] Harminder Singh Bindra1, A L Sangal2 “Investigating Performance of Extended Epidemic Routing Protocol of DTN under Routing Attack” (2014)

[26] Yinghui Guo, Sebastian Schildt and Lars Wolf COMSNETS “Detecting Blackhole and Greyhole Attacks in Vehicular Delay Tolerant Networks” (2013), Bangalore

[27] Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen “DETECTING WORMHOLE ATTACKS IN DELAY-TOLERANT NETWORKS” IEEE Wireless Communications • October 2010

[28] Fai Cheong Choo Mun Choon Chan Ee-Chien Chang “Robustness of DTN against Routing Attacks” IEEE (2010)