Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 3, Issue 5; July-September, 2016, pp. 360-365
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Improved Methods in Mitigating Misbehavior Activities in DTN: A Survey

Harveen Kaur[1] and Harleen Kaur[2]

[1]Student of Computer Science & Engineering, Baba Farid College of Engineering and Technology, Deon, Bathinda, India
[2]Department of Information and Technology, Baba Farid College of Engineering and Technology, Deon, Bathinda, India
E-mail: [1]kharveen199262@gmail.com, [2]harleengrover@gmail.com

Abstract—*DTN -Delay Tolerant Network is a special network which is suitable for sparse adhoc network unlike other wireless network it does not demand for end to end node connectivity. This is based on Bundle protocol. Bundle contains user data/information which is transmitted to destination with the help of intermediate nodes through store carry and forward principle. As DTN creates network through intermediate ferry nodes it is prone to security attacks. To offer a broad set of DTN routing protocols the ONE simulator is designed. Numerous routing and forwarding schemes are proposed which differ in their replication strategies. DTN protocol use different kind of approach than TCP/IP for delivering the packet. DTN routing protocols are Epidemic, Prophet, MaxProp, Spray-and-wait and Rapid. Rapid is considered best in terms of delivery probability, overhead ratio.*

Index Terms*: Opportunistic Network Environment, Delay Tolerant Network, Routing.*

1. INTRODUCTION

DTN, Disruption Tolerant Network is a networking architecture where nodes do not have contemporaneous connections i.e. nodes are not always connected but have scheduled intermittent connections. It is based on Store-Carry-Forward principle. This principle is similar to postal system in which whole message (entire blocks of application-program user data) is forwarded from one node's storage place to another node's storage place along a path that ultimately reaches the destination. This facilitates more delay tolerant capabilities in DTN as compared to TCP/IP [3] Store carry and Forward principle provides communications in an unstable environment where network is subjected to long lasting delays , asymmetric data rates and high error rates most of the time.(e.g. Internet for planets etc.). The main objective of DTN Routing is to build a network with minimum delay and good delivery probability. But due to the absence of end to end connectivity DTN is more prone to integrity, authenticity, black hole and worm hole attack. The Black hole attack is the most sophisticated one that can provide attack in which node could misbehave by dropping packets intentionally.[1] .ONE - Opportunistic network Environment is specially designed simulator to offer a broad set of DTN Protocol simulation capabilities in a single framework. Opportunistic network Environment is specially designed simulator to offer a broad set of DTN Protocol simulation capabilities in a single framework. The ONE simulator is designed in a modular fashion, allowing extensions of virtually all functions that can be implemented using well defined interfaces. The main function of ONE simulator are modeling of node movement, routing and message handling. Here routing protocols are based on replication strategies i.e., the number of copies of a message are created and are forwarded. Different routing protocols used here are Epidemic Routing Protocol, Prophet , Spray and wait , MaxProp , Rapid.Routing protocol[2].

2. LITERATURE REVIEW

J.Ameen Basha and D.S Arul Mozhi, Proposed a probabilistic misbehavior detection scheme in DTN i.e. iTrust for secure DTN routing for efficient trust establishment. They introduced a periodically availability of a trusted authority (TA) to judge the nodes behavior based on the gathered routing evidence. TA ensures the security of DTN routing at reduced cost. They had modeled an inspection game that showed an appropriate probability setting which assured the security of the DTN with a overhead detection.[1]

Shally et. al., Checked the performance of different routing protocols under different number of black hole attacking nodes. The analysis indicates that there is decrease in delivery probability, hop count average and buffer time average. The overhead ration increases using spray and wait protocol but decreases if rapid protocol is used upon increasing the black hole attacking nodes[2]

Ms.Aarthy D.K., Mr.C.Balakrishnan, Proposed a method to mitigate routing misbehavior proposed scheme. The scheme proposed requires the each node to maintain a signed communication report (CR), which are encrypted for security reasons. The contact node maintains CR on contacting a node when it come across another ferry node. It detects misbehaving node it convert it into legitimate node to avoid the wastage of system resources.[3]

Yinghui Guo et.al., Proposed a misbehavior detection system to defend against black hole and gray hole attacks. They evaluated a method through extensive simulations with different routing protocols. Their approach efficiently detected even nodes with low energy consumption, low false positive rate and high detection rate. When there are 30% of black hole attacker node in system, system achieve energy saving of 71%, 73%, 59% for Epidemic, Prophet and MaxProp routing protocols respectively.[4]

Qinghua.Li and Guohong.Cao, Proposed a scheme to deal with malicious node which drop packet and also may misreport to hide its misbehavior. Here, every node carry record of its previous contacts. Contact records deal with the information of time when contact happened, packets present in buffer before data exchange and which packet they receive or send during contact process. Every node report with it to the contacted node which will verify if it has dropped packets since their previous contact. Witness nodes detect misreporting node by verifying two inconsistent record it receives. This distributed scheme efficiently detect malicious node and reduce the data traffic to such nodes.[5]

Harminder Singh Bindra and A.L.Sangal, Checked the performance of three different routing protocols Rapid , Epidemic and Prophet protocol against varying message TTL.ONE Simulator to check the performance of three metric delivery probability, overhead ratio and average latency for three protocol and rapid protocol gives best performance.[6]

Garima Gupta et.al., Showed the impact of presence of black hole nodes on Dynamic Social Grouping (DSG) and then presents three algorithms to mitigate black hole attacks. The first algorithm mitigates non- collaborating black hole attacking nodes, the second algorithm that handles collaborating black hole nodes, third algorithm handles collaborative black holes as well as internal attacks.[7]

Yanzhi Ren et.al., Proposed a mutual correlation detection scheme for addressing harmful insider attack, it takes transitive property to calculate the packet delivery probability of each node and compare the information with other nodes. The evaluation of approach is done through random wave point and zebra net mobility models, the result shows MUTON can detect insider attacks with high detection rate and low false positive rate effectively.[8]

Y.Ren et.at., In this paper, a mutually correlated detection scheme is introduced by using ferry node and transitive property. Every ferry node has tables to store information of encountered node i.e. Delivery encounter table, Delivery probability table and Transitive information table. These table collect packet delivery probability of encountered node and past encounters history records of that node. The collected information verifies the change in delivery probability to other node by using transitivity property. Result shows that delivery probability claim malicious node with lower false positive rate and with reduced detection time.[10]

Y.Ren et.al., In this paper the scheme used is that node generate two tables for storing records; Receiving record table and Self record table which provide history packet records to the encountering node, these nodes check and analyze the records to decide the normality of this node. The result of the simulation shows that this method can decide insider attacks with high detection rate and low false positive. [11]

Ari Keranen et al., This simulator provides visuals of simulation interactions in real time and provides results after their completion .Its framework is a java based tool .It is featured with top section to pause, step fast forward the simulation, main section shows the complete simulation over a path where a node movement ,message handling among them are displayed, right section provides buttons to inspect each node, lower section provides log records . Generic support for DTN simulation using ns-2 and OMNet++ is fairly limited because of the limited support for DTN routing protocols.[12]

L. Feng et al., Examined the impact of the blackhole attack and its variations in DTN routing. They introduce the concept of encounter tickets to secure the evidence of each contact. In their scheme, observations that are based on the collected encounter tickets helps nodes in adopting a unique way of interpreting the contact history. Then, following the Dempster-Shafer theory, nodes form confidence opinions towards the fitness of each encountered forwarding node. To support the effectiveness of their system the extensive real-trace-driven simulation results are presented.[14]

Aruna Balasubramanian et.al., This paper provides DTN routing protocol known as resource allocation protocol for intentional DTN routing. An optimizing approach is deployed at every node. Every packet's utility is determined at every transfer opportunity that indicates which packet should be replicated to justify the network resources such as minimizing average delay, missed deadlines and maximum delay. This suggested protocol out performs incidental MaxProp routing, Spray and wait.[15]

John Burgess et.at. This paper presents a MaxProp protocol which considers hop counts in packets as measuring unit to decide transmission priority to packet. This provides the estimate of delivery likelihood. A particular threshold value is set after each transfer opportunity. Buffer space is logically split into two parts. Packets with hop count less than threshold hops are sorted by hop count and other packets with hop count less than threshold are sorted by delivery likelihood. MaxProp provides an effective protocol as it intelligently schedules packets for transmission and delete packet upon low buffer space.[16]

Thrasyvoulos Spyropoulos et.al., This paper presents a spray and wait protocol which partially behaves like epidemic protocol and rest of the time with direct transmission strategy. It doesn't keep network information or of any past encounters and results into optimized protocol when these are unknown. It has two modes of working Normal and Binary mode. Each with two phases spray phase and with phase. In spray phase, source node starts with L replicas of message which transmit [L⁄2] to replicas to the first encountered and keep rest [L/2] for itself. If replica is not reached at destination i.e. after wait phase it switches to direct transmission. It overcomes the shortcomings of purely flooding based scheme like epidemic routing protocol. It provides better performance in transmission and delivery as compared to Epidemic, utility flood , random flood, seek and focus routing strategy.[17]

*A.Vahdat et.al.,*In this paper Epidemic protocol is defined where a source node creates replicas of message and it simply forwards to all encountered nodes. The encountered node keeps the copy of message if it has buffer space and if a copy of message is not present in the node. It doesn't need predefined network information to retransmit replica of the message and past encounters of node. This protocol yields good delivery probability but overhead gets high due to utilization of buffer space.[18]

A. Routing Protocols in DTN

The different routing protocols differ in their replication policies.The routing protocols in DTN requires each node to buffer a packet in its memory and then transmits packets selectively to the ferry nodes based on various parameters i.e. the previous encounters and the estimated packet delivery probability to other nodes[16]

The various routing protocols are described below:

1. Epidemic protocol : In Epidemic protocol the messages are replicated and these replicated packets are sent to other nodes until the maximum hop count is reached, here overhead is more due to excessive utilization of storage space besides it results in good delivery probability.[2]

2. MaxProp protocol : In MaxProp protocol packets in the buffer are prioritized on the basis of various factors like hop count value , delivery probability etc. In MaxProp protocol a threshold value is decided .If the packets with the hop count less then the threshold exists they are sorted according to the hop count and are transmitted first and these packets are transmitted in increasing order .The packets which have hop count greater than the threshold value, packets are sorted by delivery likelihood these packets are deleted first in decreasing order in case of full buffer.[13]

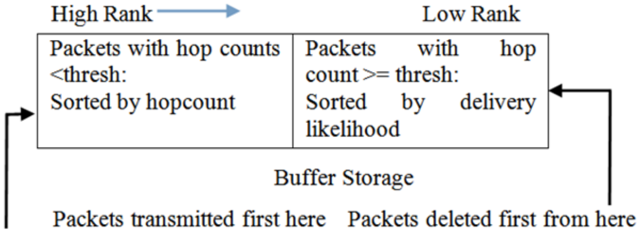
High Rank
Low Rank
Packets with hop counts <thresh:
Sorted by hopcount
Packets with hop count >= thresh:
Sorted by delivery likelihood
Buffer Storage
Packets transmitted first here
Packets deleted first from here

Fig. 1: MaxProp Routing Strategy[13]

Prophet Protocol : Prophet protocol is predictive in nature. It uses the knowledge obtained by the ferry node about its past encounters. It sends the packet to the encountered node based on delivery probability. Its delivery predictability increases as it encounters nodes and decreases exponentially. The delivery predictability also has a transitive property for the nodes which rarely meets.[8]

Spray-and-wait protocol: Spray and wait has two phases spray phase and wait phase. In spray phase a source node generate message copies and forward them. In wait phase if the destination is not found in the spraying phase each of the node carrying a message copy will directly transmit it to the destination. It has two modes normal mode and the binary mode. Binary mode has different transmission method here source node initially creates n fixed number of copies. A node that has more than one message copies and encounters another node with no copy , the first node hand over to the second node n/2 message copies and keeps rest n/2 message copies for itself , when it is left with only one copy it switches to the direct transmission.[17]

Rapid protocol : Rapid protocol is an opportunistic protocol which replicates a copy according to per packet utility function from routing metric of node i.e. it replicates a packet that increase the delivery probability locally. Specific metric are used to infer replication. The three metric it uses to infer the utility of a packet are minimizing average delay, Minimizing missed deadlines and minimizing maximum delay. It has three core components which are selection algorithm, a control channel and an inference algorithm. The selection algorithm selects the packet which it should replicate. The inference algorithm estimates the utility of a packet from the routing metric. The control channel convey the necessary meta data used in the inference algorithm. This algorithm results in minimum average delay of packet. [15]

B. Security Threats

Misbehavior in routing can drop or modify the received packets instead of forwarding to the next node. The recent researches showed that routing misbehavior leads to less packet delivery rate.[1] Some of the security vulnerabilities in DTN are:

1) Worm hole attack: In this attack the malicious node receives bundle (packet) and extracts the valuable information/data, and then re-sent it to the network in the absence of security operations. The routing protocols have a significant impact on the normal routing operations

2) Denial of service attack: The latencies in DTN are sometimes longer to allow the attacker to access the network and thus creating the possibilities of DOS attack and in return making the resources unavailable to the valid node.

3) Sybil attack: The probability of occurrence of this type of attack is high. Here the attacking node generate more than one identity to enter into the network so as to spoof it.[19]

4) Black hole attack: In this attack malicious node advertises itself as a normal node and grabs the received packets and instead of forwarding it to the next node it drops the packets thus it will effect probability of routing the packet to the destination node. Black hole nodes do not send the replicated messages i.e. the message forwarded to the node, delete it from the buffer rather forwarding it to another node. According to researches such a black hole node can effect the delivery probability, hop count average , buffer time average and overhead ratio. [10]

Gray hole attack: In this attack node switches its behavior form correct node to a bad node. To perform its malicious behavior the attacking node uses its on and off periods to perform attack which is more adverse than the continuous attack[10]. This shows a contradicting behavior from black hole attack which does not use on and off periods to perform attack, in black hole attack the node which becomes one malicious will stay malicious.

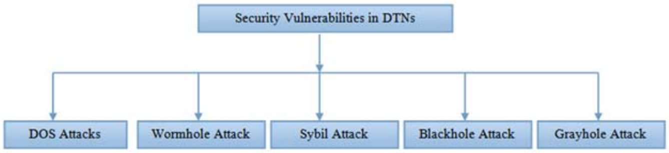

Fig. 2: Security Vulnerabilities in DTN [19]

3. DISCUSSION

Each research differs from other in terms of techniques used and the results obtained on applying them are different and thus can be compared, the following table contains the comparative analysis of papers on the basis of techniques used and results obtained.

Table 1: Table Comparative Analysis

Ref - erence no.	Author	Technique Used	Results
[1]	Ameen Basha and D.S Arul Mozhi	A probabilistic misbehavior detection scheme for secure DTN routing ,iTrust.	iTrust scheme reduce the detection overhead effectively.
[2]	Shally et. al.	ONE Simulator is used to compare spray-and-wait protocols under Black hole attack.	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.
[3]	Ms. Aarthy D.K., Mr. C. Balakrishnan.	Each node maintain a signed communication report(CR) which is encrypted to avoid forgery and helps in detecting the misbehaving node.	Detecting attacker node is done efficiently and technique can effectively mitigate routing misbehavior.
[4]	Yinghui Guo et.at.	Misbehavior detection system (MDS) is evaluated using three metrics i.e detection rate, false positive rate and energy consumption for four protocol i.e Prophet, Epidemic ,MaxProp and Spray-and-wait.	MDS achieve a high detection rate and low false positive rate for different scenario where the numbers of malicious node, the attack intensity or employed routing protocols are varied.
[5]	Qinghua Li and Guohong Cao	Distributed scheme in which a node keep a few sign records of its previous contacts and report its previous contact records to the contacted node. Based on these records detects the sanity of the node.	The detection scheme effectively detect packet dropping node locally from the contacted information and also detect misreporting when some node conspiring misreporting.
[6]	Harminder Singh Bindra and A.L. Sangal	ONE Simulator to check the performance of three metric delivery probability, overhead ratio and average latency for three protocol Rapid, Epidemic and Prophet protocol. Against varying message TTL.	Rapid protocol gives best performance.

[7]	Garima Gupta et.al.	Three algorithms are designed to mitigate black hole attack.	Detected the internal and the external black hole nodes.
[8]	Anders Lindergren et.al.	Unlike epidemic routing protocol it routes the packet by considering the delivery predictability. Which is calculated using three parts: 1)Node often encountered has high delivery predictability. 2)Predictability decreases exponentially with the time. 3)Transitivity mechanism for the two nodes which rarely meets.	Provides communication opportunities with lower communication overhead and better performance than the epidemic routing.
[10]	Yanzhi Ren et.al.	Mutual interrelationship detection scheme(MUTON) for detecting insider attack.	MUTON can detect inside attack effectively with high detection rate and low false positive rate.
[11]	Yanzhi Ren ,Mooi Choo Chuah et.al.	Two tables are generated at each node: Receiving Record table and Self Record table. When two nodes meet each other they will record the number of packets exchanged between them.	This method detects the insider attack efficiently with low false positive rate and high detection rate.
[12]	Ari Keranen, Jorg Ott, Teemu Karkkainen.	Java based tool provides simulation environment for delay tolerant network and also offer implementation of routing and application protocols. Node movement is implemented by movement models.	Provides interactive visualization and post processing tools. Reports are generated by report module.
[14]	L.Feng, W.Jie, and S.Anand.	Concept of encounter tickets is used which are generated when two nodes meet each other it holds the time stamp value. So contact history competency evaluation aging helps in calculating the forwarding decisions.	This technique hampers attackers from boosting advertising their routing metrics and yields efficient results.
[15]	Aruns Balasubramanian et.al.	Rapid protocol calculates per packet utility function from the routing metrics and selection algorithm will finally determine which packet to replicate during intermediate connectivity between two nodes.	It yields the significant performance increase for several metrics over many existing protocols.
[16]	John Burgess et.al.	MaxProp prioritize the transmission of packet to other peer node based on hop count value of packet and particularly fixed threshold value.	It performs better than protocols that have access to an Oracle which have information about the schedules of meetings between two nodes.
[17]	Thrasyvoulos Spyropoulos et.al.	Spray and wait reduces the overhead involved in flooding based scheme by limiting the forwarding of message using their specific spray phase and wait phase.	It out performs epidemic protocol. It reduces average message delivery delay, increases packet delivery probability and reduces overhead.
[18]	A.Vahdat and D. Becker	It is based on flooding based scheme where a node keeping replica of a message forwards forward all its replica to every connected node in case of absence of that message in the node.	Provides good delivery probability but high overhead.

4. CONCLUSION

DTN-Delay Tolerant Network are basically used in sparse adhoc network. It is used to increase the delivery probability. Unlike TCP/IP it does not demand end to end connectivity. Various routing protocols are classified according to their replication strategies. Discussed scenarios concludes Rapid routing protocol giving good delivery probability and overhead ratio which decreases but after a limit it increases. In future performance evaluation of other routing protocols in various adverse scenarios will be discussed.

REFERENCES

[1] Ameen Basha and D.S Arul Mozhi, "Detection of Misbehavior Activities in Delay Tolerant Network using trusted authority,2014" ISSN:2321-9939 2014 IJEDR.

[2] Shally, Harminder Singh Bindra, Mamta Garg, "Performance evaluation of rapid and spray-and-wait DTN Routing protocols under Black hole attack" eISSN:2319-1162 2014 IJRET.

[3] Ms.Aarthy D.K., Mr.C.Balakrishnan "Detecting Selfish Routing and Misbehavior of Malicious Node in Disruption Tolerant Network" ISSN 2250-24592013.IJETAE.

[4] Yinghui Guo, Sebastin Schildt and Lars Wolf., "Detecting Black hole and gray hole attacks in Vehicular Delay Tolerant Network" 2013IEEE.

[5] Q.Li and G.Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks" IEEE Transaction on Information Forensics and security,Vol.7,No.2,April 2012.

[6] Harminder Singh Bindra and A.L.Sangal, "Performance Comparison of Rapid, Epidemic and Prophet routing protocols for Delay Tolerant Network" International Journal2012.

[7] Garima Gupta, Preeti Nagrath, Sndhya Aneja, Neelima Gupta, "Reference Based Approach to Mitigate Black hole Attacks in Delay Tolerant Networks." ACM 2012.

[8] Anders Lindgren, Avri Doria, Olov Schelen, "Probabilistic Routing in Intermittently Connected Networks" SIGMOBILE Mobile Computing and Communications Review, 7,2003.

[9] N.Li and S.Das, "A Trust-based Framework for Data Forwarding in Opportunistic Networks" Ad hoc Networks, 2011.

[10] Yanzhi Ren et.al. "MUTON: Detecting Malicious node in Disruption Tolerant Network" 2010. IEEE.

[11] Y.Ren, M. Chuah,j.Yang, and Y.Chen, "Detecting Blackhole Attacks in Disruption Tolerant Networks through Packet Exchange Recording" In Proceedings of IEEE International Symposium on A World of Wireless Mobile and Multimedia Networks(WoWMoM),Pages1-6,2010.

[12] Ari Keranen, Jorg Ott, Teemu Karkkainen, "The ONE Simulator for DTN Protocol Evaluation" In The Proceedings of the 2nd International Conference on Simulation Tools and Techniques, SIMU Tools O09,2009.

[13] N.Bhutta, G. Ansa, E.Johnson, N.Ahmad, "Security Analysis for Delay Slash Disruption Tolerant satellite and Senson Networks" Satellite and Space Communications, IWSSC2009,International Workshop,pp-385-389.

[14] L.Feng, W.Jie, and S.Anand, "Thwarting Blackhole attacks in Disruption Tolerant Networks using Encounter tickets", In Proceedings of IEEE INFOCOM Pages 2428-2436, March2009.

[15] Aruns Balasubramanian, Brian Neil Levine and Arun Venkataramani, "DTN Routing as a Resource Allocation Problem" 2007 ACM.

[16] John Burgess, Brian Gallagher, David Jensen, Brian Neil, Levine, "MaxProp: Routing for vehicle based Disruption Tolerant Networks" 2006

[17] Thrasyvoulos Spyropoulos, KonstantinosPsounis, Cauligi S.Raghavendra, "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks" 2005 ACM.

[18] A.Vahdat and D. Becker, "Epidemic Routing for Partially-Connected Ad hoc Networks" Technical report, Duke University, 2000.

[19] Contemporary Survey of DTN Security Available at "http://web.nmsu.edu/~chssrk/" Last accessed on April 19, 2015.