Mitigating Black Hole Attacks in Opportunistic Routing for Delay Tolerant Networks

A. R. Naseer, *Senior Member, IEEE* and A. Saichand, *Member, IAENG*

***Abstract*— Mitigating routing misbehavior due to insider attacks in Delay Tolerant Networks is very crucial as Delay Tolerant Networks (DTNs) are deployed in battlefield environments and emergency situations to provide critical services. The effect of insider attacks cannot be tackled with traditional approaches as DTN characteristics are different from ad hoc and other wireless networks, wherein connectivity among mobile nodes is not always guaranteed. In this paper, we propose a solution to mitigate Black Hole(BH) attacks in DTNs by segregating the simple information like sent and received packets to and from multiple nodes. We evaluated our approach through OMNeT++ simulation using Random Way Point model. Our results show that our approach can mitigate black hole attacks efficiently with high detection rate.**

***Index Terms*— Black Hole attacks, Routing Misbehavior, Opportunistic Routing, Delay-Tolerant Networks, Intermittently Connected Mobile networks, Delay Disruption Networks, Socially Aware Opportunistic Routing**

I. Introduction

Unlike Traditional networks, Delay Tolerant Networks (DTNs) are wireless networks where fully connected path is unlikely to exit between source & destination all the time. They are also referred to as Intermittently Connected Mobile Networks or Delay Disruption Networks where routing is decided in an opportunistic fashion for message delivery and nodes in these networks use store-carry and -forward strategy to route the messages. Due to the mobility of most of the nodes in DTNs, network connectivity is achieved by nodes using contact opportunism i.e., only when these nodes come into the transmission ranges of each other. If a node has a copy of the message to forward and is not connected to another node, it stores the message and carries it until a suitable contact opportunity arises. DTNs cover a class of highly partitioned networks that suffer from frequent dis-connectivity & long delay which include wireless sensor networks using scheduled intermittent connectivity, terrestrial wireless networks with no end-to-end connectivity, satellite networks with long delay or periodic connectivity, underwater acoustic networks with frequent interruptions, military networks, vehicular ad hoc networks, etc. Dynamic Change in network topology and lack of end-to-end connectivity pose a number of routing challenges for Delay Tolerant Networks. Several routing algorithms have been proposed in the literature for DTNs to guarantee messages delivery even in the presence of network partitions. Some of the major classes of DTN routing algorithms are Epidemic based, Probability based and Social Structure-aware based routing approaches. In Epidemic - based methods, multiple copies of the same message is transmitted with the hope that at least one reaches the destination. In probability based approaches, the sender forwards the message to the node having the highest probability of successful message delivery. In social structure-aware routing algorithms, message exchanges between nodes are performed considering the social relations of nodes.

Mitigating routing misbehavior in Delay Tolerant Networks has been an active area of research. Routing misbehavior can be caused by malicious nodes (e.g. Black hole nodes) that drop packets intentionally or modify the packets to launch insider attacks or Selfish nodes that try to conserve its own resources by refusing to cooperate in packet forwarding for others. Malicious and selfish behaviors of nodes will significantly reduce the packet delivery rate and thus pose a serious threat against the network performance of DTNs. The Black hole (BH) node is a malicious node that involves in routing path during route discovery by announcing that it has the best route to the destination and drop packets during data transmission. Whenever a node wants to send data to the destination, it will send route request(rreq) to its neighbors. The neighbor which has better metric than the sender will send the route reply(rrep) to the sender. The sender will select the best one from all the rreps and send the data to that particular neighbor. A black hole node will receive the route request packets and sends the reply by keeping best metric in route reply to the destination. As it announces the best metric, it is obvious that the black hole will be selected as the next node. After receiving the data, it will not generate the route request and it will not forward packets. Further, it will simply drop the packets. The solutions that work well for ad hoc networks will not work for DTNs as they have different network characteristics [1] compared to ad hoc networks. Average number of neighbors of any node in DTN is less compared to that of the ad hoc networks. In this paper, we are proposing an approach for mitigating Black hole Attacks in Socially Aware multiphase opportunistic routing proposed in [2]. Our proposed approach to mitigate black hole attacks is an enhancement to packet exchange recording method [3]. When compared to packet exchange recording, our method will detect black holes within less time because the tables are propagated through beacons. Moreover, number of times the

Manuscript received March 20, 2016; revised April 4, 2016.

A. R. Naseer is Principal & Professor at the Department of Computer Science & Engineering, Jyothishmathi Institute of Technology & Science (JITS Karimnagar) affiliated to Jawaharlal Nehru Technological University(JNTU), Hyderabad, Telangana State, India (corresponding author - phone: +91 9052430745; e-mail: dr_arnaseer@hotmail.com).

A. Saichand was with the Department of Computer Science & Engineering, JITS Karimnagar affiliated to JNTU Hyderabad. He is now Assistant Manager(Systems)-IT Specialist Officer, State Bank of India, Administrative office, Hubli, Karnataka State, India (email: amirishettisaichand@gmail.com).

black hole detected is also more than the packet exchange recording.

The rest of the paper is organized as follows. In Section II, we present some of the previous work related to black hole attacks in opportunistic networks. Section III presents our proposed approach for mitigating both passive and active black hole attacks in opportunistic routing for DTNs. The simulation setup, network performance before and after the presence of both passive and active black hole nodes without and with the application of our mitigation approach are presented in the Results and Discussion Section IV, followed by Concluding remarks in section V.

II. Related Work

In this section, we present some of the previous work related to black hole attacks in opportunistic networks.

In packet exchange recording [3], when any two nodes meet each node will generate 2 tables one for itself called as SRT (Self Record Table) and the second table RRT (Receiving Record Table) for storing in the other node that it will send it to the other node. For example, when 2 nodes A and B meet, node B generates a packet record that will be stored in RRT of node A with the following information - ids of node A and node B, number of receiving packets from node B, number of sent packets to node B, current time stamp. The node B signs this record with its private key. Similarly, node A will generate a packet record that will be stored in RRT of node B. The node A signs this record with its private key. RRT of B contains the following information- ids of node A and node B, number of receiving packets from node A, number of sent packets to node A, current time stamp. Whenever a node meets other node, it stores id of other node and Encountering time in its *SRT*. When node A encounters node B, node A requests node Bs RRT, with that node A calculates packet forwarding percentage of node B. With that value, A can decide whether to select node B as next hop or not. To exhibit better ratio, node B can drop some of the entries of RRT. Node A can detect this by comparing the entries of RRT with its own SRT and RRT. But node A can detect this situation only if B deletes the entries of node A (when node B meets with node A, node A will store record in Bs RRT). If it is the first time that node B is meeting node A then it will not have an entry regarding node A and always it may not be the case that in the deleted list of B node A entry will be there.

In [4] the authors explored the issue of selective dropping. In this some nodes are being used as trusted nodes to monitor their neighbors. This method will not be applicable to DTNs as each node will not have enough neighbors to monitor. In [5], the authors introduced the periodically available trusted authorities depending on previous routing patterns and probabilistic checking. In [6] the behavior of the node is found out by collecting the information from neighboring nodes and combined faith value is calculated. Depending on this value, the node is treated as valid or invalid. [7] Proposes that nodes encounter probability is not an appropriate measure of the nodes delivery probability. They proposed a trust based frame work to evaluate nodes delivery probability.

In [8] authors propose a cluster based detection scheme where one of the nodes of the cluster is elected as cluster head, it has to listen to its neighbors and by comparing the gathered information with predefined metrics, it will detect the abnormality. But in sparse DTNs, number of neighbors a node can detect is very less.

A ferry based detection method (FBIDM)[9] is proposed on the concept of trusted examiner which is called as ferry node. Each ferry node will gather the information about its associated neighbors and is responsible for finding the abnormality. But in this method delivery probability calculation does not include the transitive property. MUTON [10] proposes an improved ferry based detection method which includes transitive delivery probability. However, the usage of ferry nodes incurs additional overhead on the network. [11] uses contact history by using encounter tickets to find out the abnormality. But they have not proposed any solution for packet dropping in black hole attacks.

III. Proposed Approach

In this section, we propose a solution to mitigate black hole attack in opportunistic routing that uses between-ness [12] as metric. Mitigating approach for tackling black hole attacks can be considered as dealing with passive and active nature of BH nodes. Passive black hole is a compromised node that would not change the metrics i.e. it does not attract the senders, if selected it will receive the data but it will not send it further. Active black hole means it actively participates i.e. it will change its metric to high value and attracts the sender. There will be more data loss with active black hole than passive black hole. For providing solution to either passive or active nature of black hole attacks, our method maintains Sent Table (ST) and Receive Table(RT) at each node. Sent Table and Receive Table store the number of packets sent by the particular node to other nodes and the number of packets received by the node from other nodes respectively. For example, node A has received 3 packets from node B, 2 from node C, 5 packets from node D and node A has sent 4 packets to node B, 3 packets to E then the ST and RT will be as shown in table 1.1 and table 1.2.

Table 1.1. Node A Sent Table

Node Id	Sent Packets
B	4
C	0
D	0
E	3

Table 1.2 Node A Receive Table

Node Id	Received Packets
B	3
C	2
D	5
E	0

Whenever a node sends or receives a packets, it will update the ST and RT. These ST and RTs will be exchanged by beacons. Each node will store other nodes' STs and RTs along with its own ST and RT. When a node wants to send the route reply (rrep), it has to send its ST and RT along with the rrep. The sender will receive the rrep, ST and RT table of the rrep sending node. After receiving, the node will check incoming ST with RT of the corresponding node in master SRT(Send Receive Table) and incoming RT with ST of the corresponding node in the master SRT table.

A. Approach for Passive Black Hole Attacks

Solution for passive black hole is simple compared to that of active. As the node is not going to change the metric and its tables ST and RT, we can check whether the node has

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

sent any packets by looking at sent table. The sender will get the data about sent table and receive table from route reply. Tables in the route reply provide sufficient information to check whether the replying node is BH or not. So there is no need to load the ST and RT tables of the beacon messages in to network SRT. The sender node which receives the rrep will check whether the replying node sent table and receive table have some entries. Table 2 provides different cases of solution and conclusions that can be made from the sent table and receive table of the replying nodes.

Table 2: Different Cases of Solution

Cases	Sent and received tables in rrep packet	Conclusion made at the receiver of rrep
Case1	Size of sent table > 0 and size of receive table>0	It resembles that node has sent some packets to other nodes, replying node not treated as BH.
Case2	Size of receive table=0 and size of sent table =0:	It indicates that it has no packets to send so we cannot decide whether replying node is a BH or not.
Case3	Size of receive table>0 and size of sent table=0	In this the node has received the packets but it has not sent those packets there may be 2 reasons it may be a BH or it has not found any node that has better metric.
Case4	size of receive table=0 and size of sent table>0	not possible

In the first case of solution, sender will not send packets if the sent table of replying node has no entries and if received table has some entries. We may have more *false positives*, that is normal node can be detected as black hole. If the replying node is not a BH and it is trying to find a better relay then also it will be detected as BH. If the received table size=0 then we are treating that node as a normal node as we do not have sufficient info to judge the node, here we may have *true negatives*, that is, a BH node can be treated as a normal node. For reducing false positives, we are implementing a timer based mechanism where we note the time at which the replying node has stored the packets in the receive table, from that time we will keep some time limit till that time limit that node cannot be treated as BH. If after the time limit also, no entries are in the sent table then we treat that node as BH. For reducing true negatives, only option available is we have to wait until the node receives some packets.

B. Approach for Active Black Hole Attacks

In the case of active black hole, route reply sending node will modify its metric, i.e., number of packets sent or received in sent table and or received table. That is, even if it has not sent any packets it will add some entries in the sent table to resemble that it is not a BH. Now the sender or rrep receiving node will not be able to judge the replying node by examining its information. In order to find out whether the entries in the ST and RT of the replying node are genuine, the sender will take the information from other nodes by using beacons. That is, the sender will store the ST and RT of the nodes which it encountered recently using beacons. If these nodes also encountered the replying node, they will have corresponding entries in their tables. These tables will be cross checked with ST and RT of the replying node at the sender. If any mismatch is found then we can decide that the replying node is a BH. So this method requires that every node has to put ST and RT as part of beacon massages as well as rreps.

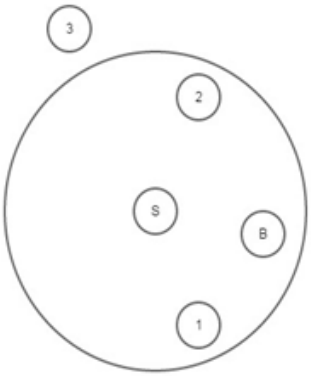

Figure 1. Example Network

Table 3: Node 1 ST and RT

Node Id	Sent Packets		Node Id	Received Packets
B	5		B	0
2	3		2	2
3	2		3	4

Table 4: Node B ST and RT

Node Id	Sent Packets		Node Id	Received Packets
2	4		2	0
1	0		1	0
3	0		3	2

Table 5: Node 2 ST and RT

Node Id	Sent Packets		Node Id	Received Packets
B	0		B	0
1	5		1	3
3	2		3	5

For example, consider the figure1, node S is the sending node, nodes 1, B and 2 are its neighbors. Node S will send the rreq to 1, B and 2. As node B is the black hole node, it will send the rrep (by keeping better metric), its ST and RT to node S. But as the node B is a black hole node, it will have zero number of packets in its sent table, which indicates that it will not be selected as next hop.

In order for the node to be not detected as BH, node B can modify its ST and RT in 2 ways.

- To increase number of sent packets, Node B can modify its number of sent packets by keeping some value even though it has not sent any packets.

  The change of sent packets can be handled at S node by comparing the sent column of ST of node B with received column of other nodes RTs which it received through beacons. For example, considering the figure1 and table4, node B has shown in its sent table that it has sent 4 packets to node 2. Where as in table 5, the received RT of node 2 it has shown that node 2 has received 0 packets from node B, here we can decide that

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

node B is BH.

- To decrease the number of received packets, it can modify the number of received packets to 0, even though it has received packets from other node so that it can pretend that it has not received any packets, that's why it has not sent any packets.

  The change of received packets can be handled by comparing replying node RT entries with entries of other ST which it received using beacons. For example, considering table 4, if node B modifies the number of received packets from node 1 to 0, it can be found out by comparing the sent column of node 1(table 3) that has node id B, which shows that it has sent 5 packets to node B so we can decide that node B has modified the received table and we can conclude that node B is BH.

The process flow of the proposed solution is depicted in figure 2.

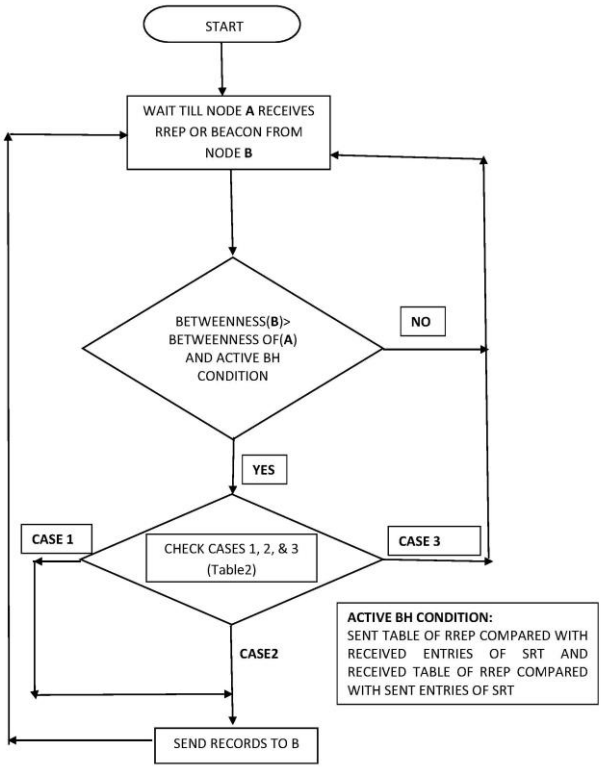

Fig. 2 Process flow of the Proposed Solution

C. Opportunistic Routing Protocol Used

In this work, we have applied our approach of mitigating Black Hole attacks to SAMPhO[2]-Socially Aware Multi Phase Opportunistic routing with Radom way point mobility model. The working principle of SAMPhO can be described in terms of phases. A phase in the opportunistic routing procedure is defined by the different social conditions in the carrier's physical neighborhood.

The phases of Opportunistic routing procedure are :

- Contemporary ad-hoc delivery phase.
- Centrality-based forwarding phase
- Copy spreading phase.
- Probability-based forwarding phase.

- *Contemporary ad-hoc delivery phase* – In this phase, the immediate delivery of a message is achieved through an existing path using ad-hoc routing mechanisms.

- C*entrality-based forwarding phase* - This phase is used when the destination is not reachable by the source and no social information exists with the neighbors which means that the destination is far. In this phase, the messages should be routed using global centrality metrics (e.g. betweenness).

- C*opy spreading phase* - In order to detect the destination, a network of central nodes is required to spread the message throughout the whole network. Central nodes copy messages between them thereby trying to detect the destination.

- *Probability-based forwarding phase* - After destination is detected by one of the central carriers, messages can be forwarded according to the node which has the higher probability of contacting the destination.

As evident in [2], these phases do not occur always in an ordered fashion, but can appear interchangeably and multiple times. In many cases, a message does not need to pass from all of these phases to be delivered. For example, a packet can fall from the centrality-based forwarding stage straight to the probability-based forwarding.

IV. Results and Discussion

A. Simulation Setup

The system was implemented using the OMNET++ simulator and the INET/MANET frameworks. The simulations involve a network of 30 nodes. The total duration of the simulation was 42200 seconds. The simulation area was 4*km* × 4*km*. Each node is randomly placed into the grid. Nodes start transmitting messages to random destination during the [35000,38000] simulation time interval, with an approximate rate of 36 messages per hour. That is, for every t_m seconds node transmits one packet. After a specific point in time T_{start}, each node begins to generate messages every T_m seconds towards random destinations. This traffic generation model simulates a distributed mobile social network application. The message generation process stops at T_{stop}, while the packet size is set to 1KB. All simulation parameters are shown in table 6.

Table 6. Simulation Parameters

Simulation	**Variable value**
Simulation time	42200 secs
t_{start}	35000^{th} sec
t_{stop}	38000^{th} sec
Simulation area	4*km* × 4*km*
$t_{message}$	60 secs
No of nodes	30
Packet size	1KB
Mobility model	Random

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

In this work, we have applied our approach of mitigating Black Hole attacks to SAMPhO: Socially Aware Multi Phase Opportunistic routing with Radom way point mobility model.

B. Simulation Results of Passive Black Hole Nodes

Network performance before the presence of passive Black Holes

Under normal operation, no node is a black hole and every node is functioning normally. In this simulation scenario, the total number of received packets of all nodes is 440 as shown in figure 2.

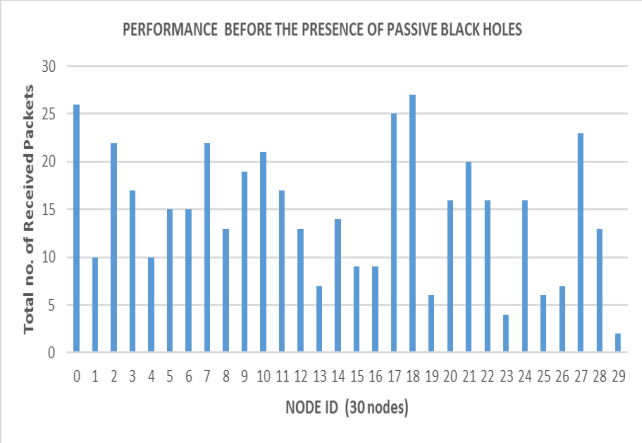

Fig 2: Total no. of Received Packets of Randomly selected Destinations

Network performance after the presence of 5 passive Black Holes without the mitigation approach

As these 5 BHs will not forward the packets further, the total no of packets received by all nodes reduces to 224 as shown in figure 3.

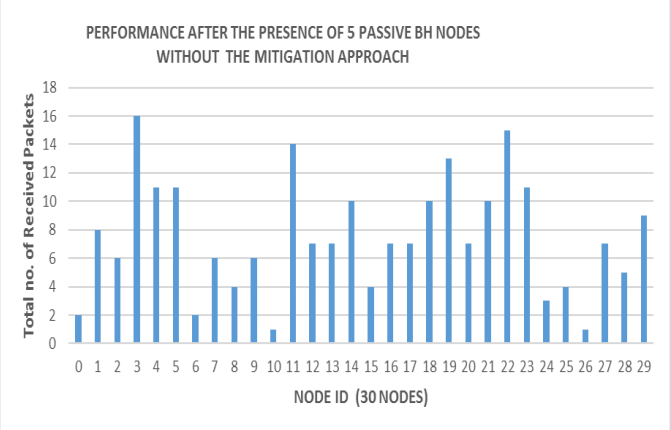

Fig 3: Total no of received packets of randomly selected destination after 5 randomly selected destinations act as Black holes

Network Performance after the presence of 5 passive BH nodes with the Mitigation Approach applied

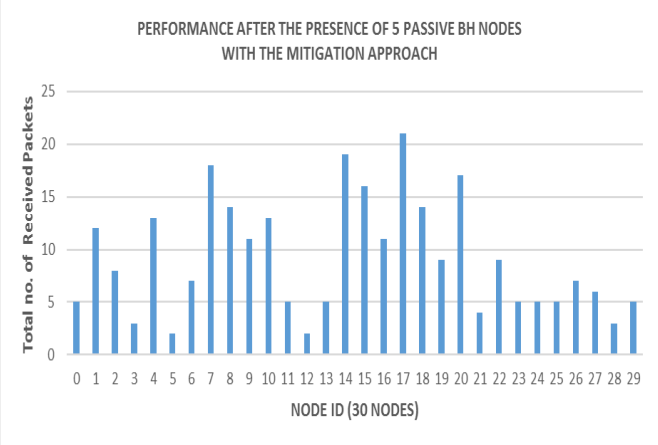

Fig. 4: Total no. of received packets of randomly selected destination after 5 randomly selected destinations act as Black holes with the Mitigation Approach

With the proposed Mitigation approach applied to Network with 5 nodes acting as passive BH nodes, the total number of packets received improves to 274 as shown in figure 4. The results obtained shows that there is a significant improvement with the proposed Mitigation Approach. If we observe the results of figure 3, that is, without the approach, the total number of received packets by all nodes is 224. Considering figure 4, which shows the results after the passive BH mitigation, there is an improvement of 50 packets in the total number of received packets.

C. Simulation Results of Active Black Hole Nodes

Network Performance after presence of 5 active BH without the mitigation approach

The total number of packets received at the destination is less compared to the presence of passive BHs. Because always BH node will be selected as the next node as it shows the better metric. Whereas passive BH does not show the better metric. As shown in figure 5, the presence of 5 random active BHs reduces the total number of packets received from 440 to 152.

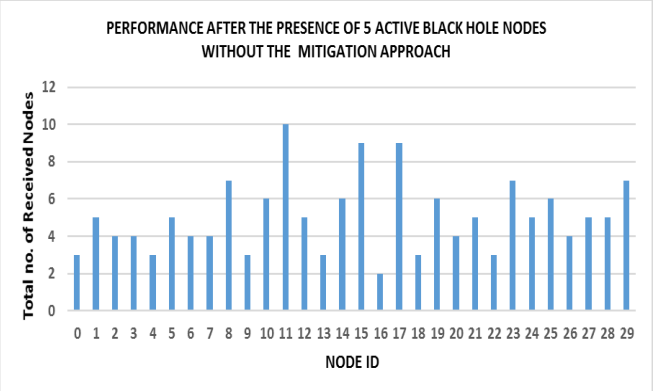

Fig 5: The Total no of received packets of randomly selected destination after 5 randomly selected destinations act as active black holes.

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Network Performance after the presence of 5 active BH nodes with the Mitigation Approach applied

As shown in figure 6, with the proposed Mitigation approach after 5 nodes acting as active Black Holes, the total no of packets received improves to 238.

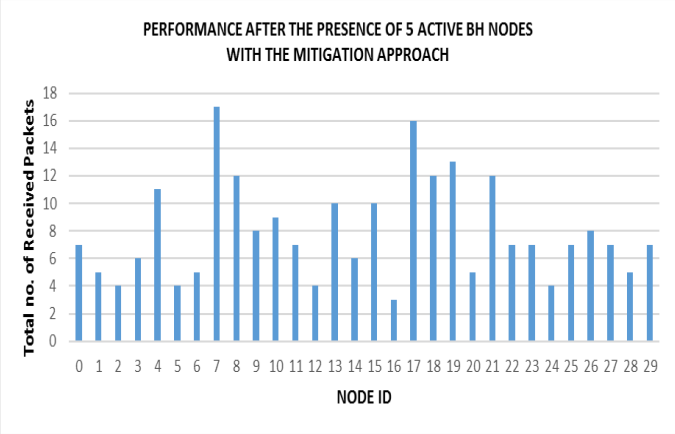

Fig. 6: Total no of received packets of randomly selected destination after 5 randomly selected destinations acting as Black holes with Mitigation Approach Applied.

With the proposed Mitigation approach applied to Network with 5 nodes acting as active BH nodes, the total number of packets received improves to 238 as shown in figure 6. The results obtained shows that there is a significant improvement with the proposed Mitigation Approach. If we observe the results of figure 5, that is, without the approach, the total number of received packets by all nodes is 152. Considering the figure 6, which shows the results after the active BH mitigation, there is an improvement of 86 packets in the total number of received packets.

V. Conclusion

In this paper, an approach for mitigating black hole attacks in socially aware multiphase opportunistic routing for Delay Tolerant Networks is presented. Our proposed approach to mitigate black hole attacks is an enhancement to the packet exchange recording method. When compared to the packet exchange recording, our method will detect black holes within less time because the tables are propagated through beacons. Number of times the black hole detected is also more than the packet exchange recording because in packet exchange recording the sender will compare only with its ST and RT where as in our method the rrep sending node's ST and RT are compared with multiple nodes' STs and RTs. With this analysis, we can conclude that our method performs better than packet exchange recording. Further, our future work includes investigation of number of true negatives and false positives in the solution and to propose suitable mechanisms to improve the mitigation process.

References

[1] S. Farrell and V.Cahill, "Delay and Disruption Tolerant Networking", Artech House Publishers, 2006.
[2] Nikolaos Vastardis, Kun Yang, "Multi-Phase Socially-Aware Routing in Distributed Mobile Social Networks", 9th International Conference: on Wireless Communications and Mobile Computing (IWCMC), 2013.
[3] Yanzhi Ren, Mooi Choo Chuah, Jie Yang, Yingying Chen, "Detecting blackhole attacks in Disruption-Tolerant Networks through packet exchange recording", IEEE 14th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2010.
[4] S. Marti, T.J.Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", 6th ACM International Conference in Mobile Computing and Networks, August 2000.
[5] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE Transactions on Parallel and distributed Systems, issue no. 01, Jan. 2014, vol. 25, pp 22-32.
[6] A. K. Gupta, I. Bhattacharya, P.S. Banerjee, J. K. Mandal, "A Co-operative Approach to Thwart Selfish and Black-Hole Attacks in DTN for Post Disaster Scenario", IEEE Fourth International Conference of Emerging Applications of Information Technology (EAIT), Dec, 2014, pp 113-118.
[7] Na Li A, Sajal K. Das, "Trust-based framework for data forwarding in opportunistic networks", Journal on Ad Hoc Networks, Vol. 11, No. 4, June 2013, pp. 1497-1509.
[8] Y. Huang and W. Lee, "A cooperative intrusion detection system for ad hoc networks", Proceedings of 1st ACM Workshop on Security of Ad Hoc Networks, 2003.
[9] M. Chuah, P. Yang, and J. Han, "A ferry-based intrusion detection scheme for sparsely connected adhoc networks", Proceedings of first workshop on security for emerging ubiquitous computing, 2007.
[10] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Muton: Detecting malicious nodes in disruption-tolerant networks,", Proceedings of WCNC 2010.
[11] Li, J. Wu, and A. Srinivasan, "Thwarting black hole attacks in disruption-tolerant networks using encounter tickets", Proceedings of IEEE INFOCOM'09, 2009
[12] Martin Everetta, Stephen P. Borgattib, "Ego network betweenness", ELSEVIER Social Networks 27 (2005) 31–38.

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)