A Co-operative Mechanism to Contrast Black-hole Attacks in Delay Tolerant Networks

[1]Shuchita Upadhyaya and [2] Karishma
[1(]*Professor, DCSA Kurukshetra University Kurukshetra)*
[2(] *P.G. Student, DCSA Kurukshetra University Kurukshetra)*

ABSTRACT: *DTNs are designed to work in post disaster scenario where partitions between nodes are large. To transfer messages in this situation DTN uses intermediate nodes to forward messages. The mechanism used here is store, carry and forward. But here, securely transferring messages from one node to other node is quite challenging task because an intermediate node may behaves maliciously. A malicious node may be a black hole, selfish node or sinkhole. This paper focuses on black hole attack. In this paper a cooperative mechanism is described in literature [6] that helps in prevention of network from black hole attack. A review of this proposition has led to an identification of modifications that can be incorporate to yield better results. These modifications are enlisted in the paper.*

Keywords: *DTN (Delay Tolerant Network), Black hole, CFV (Combined Faith Value) and encounters.*

I. INTRODUCTION

The development of delay tolerant networks has bringing up a revolutionary change in the field of wireless. It is practically possible to connect the network in a region where network connectivity seems impossible. Delay tolerant networks have intermittent node connectivity and nodes in DTN are highly mobile. Due to such unusual network behavior, DTN uses store-carry-forward model as message propagation process. In store-carry-forward model, DTN node will send message to intermediate nodes only if it gets an opportunity or only if it comes in range of other node else it elect to save the node in its buffer[1]. Also there may be possibility of long run persistent buffer storage. Sometimes, DTN nodes does not behave normally from their standard behavior and behaves abnormally intentionally tries to harm the network performance. Mostly all the networks face the problem of malicious nodes. Unlike traditional networks, it is hard to detect such type of nodes in DTN due to network inconsistency and exclusive characteristics. Malicious nodes are further divides into different categories1) selfish nodes 2) black hole nodes 3) Worm Hole 4) Sinkhole etc. This paper focused only on black hole attack. A black hole attack is an attack in which nodes silently removes or drops the entering or leaving traffic deprived of informing the source that message didn't receive destination. These nodes stay invisible in the network and are detected only when traffic lost is monitored [2].

Prevention of DTN is required from injurious possessions of black hole attack. To prevent network from black hole attack, a robust mechanism is required that contrast black hole attack [3]. It is difficult to predict a node that whether it is malicious node or normal node. For this a faith value of each node is calculated to distinguish them. This faith value should be depends on the historical performances of nodes with each other within the network. Thus cooperation between nodes is required. A node may influenced its information hence the assessment of its faith value must avoid values after obtaining from previous node.

II. RELATED WORK

Different works has been studied to get the focused and viable mechanism to detect a malicious node in DTN. Some of them are listed below. Basically the concept involved is of node history, which is manipulated in various ways. The base of this paper [6] has a cooperative mechanism to find a black hole node.

In [6] focused on neighbouring node cooperation scheme to reduce the malicious node impact on DTN post disaster scenario. Each node maintains a past experience of every other contacted node and at the time of message transmission, CFV (combined faith value) value is computed on the basis of received, sent messages then this CFV further compares with the threshold value to judge the node. Along with this, CFV value also multicast in the network for updating.

In [7] proposed a technique in which ferry nodes are used to detect malicious nodes within network. This technique was not so efficient because of dense connectivity of network also complete dependency on ferry nodes.

In [9] provides mechanism to secure network from selfish nodes but the mechanism was not so good to remove them. Also the mechanism was not able to detect black hole attack.

In [10] proposed trust based mechanism to detect black hole nodes from DTN. The proposed strategy works fine with only spray and wait routing as compare to other existing routing schemes.

In [11] proposed mechanism to contrast black hole nodes based on encounter measurement mechanism. In proposed mechanism each node maintains a record of its encounters with other nodes and these records of each node are compared by threshold value and calculate black hole nodes if nodes encounter value was less then threshold value.

In [12] proposed a reputation based algorithm to identify the impact of black hole in DTN also contrast them from networks by using cryptography. To put it plainly, after selecting the following sending node, i.e., the node to forward a message to, a node gauges how well a hopeful sending node has acted on the premise of past cooperation with that conceivable sending node. They call reputation such assessment. Practically speaking the reputation measures the dependability of a node.

In [13] authors concentrate on an assault in which a halfway node drops parcels going through it. The inspiration of the dropper node is the safeguarding of its assets, for example, its restricted battery, while in the meantime utilizing the assets of others to convey its information. It is qualified as childish node for this situation. A disavowal of administration assault can be the point of the dropper node to destruct the end-to-end correspondence. The dropper node is qualified as malignant node for this situation. To complete its assault, the dropper node should firstly be in the way between the source and the destination nodes, and then it drops parcels experiencing it. As indicated by the steering convention utilized as a part of the system, the way in which the dropper node acts is distinctive.

In [14] the impact of dark gap assault in AODV based system is examined. The system parameters like Throughput, Packet Delivery Fraction (PDF) and Average End to End Delay are computed with ordinary system (without dark opening) and a system with one dark gap. The execution of system parameters are thought about in all the three situations.

In [15] provides complete survey by examination on the best in class countermeasures to manage the parcel dropping assault. Besides, we look at the difficulties that stay to be handled by specialists for building an inside and out barrier against such a complex assault.

In [16] author present three solutions to mitigate black hole attacks. The first algorithm mitigates non collaborating black hole nodes. In the second algorithm, they presented a solution that handles collaborating black hole nodes. The first two algorithms handle only the external attacks. It does not handle the scenario in which a node that is good initially and becomes malicious or selfish later. Finally, they present third algorithm which handles collaborative black holes as well as internal attacks. They validated the performance of proposed algorithms through extensive simulation in ONE simulator.

After studying or review various researcher papers we provide literature survey of few papers as above. Each one has its own pros and cons. We choose cooperative mechanism to contrast black hole proposed by [6] because author provides detailed mechanism to detect black hole attack. In proposed scheme a CFV was computed firstly and on the basis of that value black holes are distinguished. This mechanism was much better as compare to other techniques in perspective of detection of black hole attack with high delivery ratio.

III. COOPERATIVE MECHANISM TO CONTRAST BLACK-HOLE ATTACK

[6] Proposes a cooperative mechanism to detect black hole attack. In this mechanism each node maintains their history that includes message delivery rate of that node and on the basis of this rate a CFV i.e. combined faith value is determined separately. When a sending node wants to send packet then all its neighbor nodes give their opinion about the node that was chosen by sending node to send the packet. They give their opinion on the basis of their past encounters with that node. From their opinion a faith value is obtained and then this faith value was compared with a predefined value. If the faith value was below to this minimum value then that node is black hole otherwise it is a normal node.
A CFV can be calculated by equation mentioned as below:
Here rcvd: Number of received packets.
Et: Elapsed time.
Snt: Sent messages.
Mcr: Average message creation rate.

$$CFV = 1- \{(rcvd + mcr \times et) - snt\}/(rcvd+mcr \times et)$$
$$= snt/(rcvd+mcr \times et)$$

[6]

To elaborate proposed work an example is given below:

TABLE I

CFV VALUE OF EACH NODE

Number of Nodes	Number of packets delivered	Number of packets Received	CFV value
Node A	4	6	0.57
Node B	8	5	0.65
Node C	5	3	0.87
Node D	2	6	0.81
Node E	2	11	0.74

Table I depicts calculation of CFV value of each node separately by computing number of packets received by node and number of packets sends by node.

IV. PERFORMANCE RESULTS AND EVALUATION

In this section performance of network are evaluated when black hole are present between network during packet transmission. For this performance metrics used are:

a) Dropped packets: This metric is used to count numbers of packets are dropped during simulation.
b) Delivery ratio: This metric represent the delivery ratio of nodes during simulation in network.

Performance parameters: For evaluations of proposed work black holes are varied from 0 to 50.

These simulation parameters are used in base paper. So when we propose our mechanism we use these parameter and additional parameters like overhead ratio and message delay occurred when black hole nodes increases in networks.

TABLE II

DELIVERY RATIO V/S BLACK HOLE NODES

Black hole nodes	Delivery ratio
0	0.75
10	0.6
25	0.52
50	0.1

TABLE III

BLACK HOLE NODES V/S DROPPED PACKETS

Black hole nodes	Dropped rate
0	0
10	15
25	175
50	421

Table 2 and Table 3 show the results of our base paper. The results shown delivery ratio and dropped rate occurred during data transmission when black holes are presented in network as these black holes increases then drop rate increases and delivery ratio decreases.

V. PROPOSED MODIFICATION

As earlier we discuss cooperative mechanism to detect black hole nodes in DTN. This scheme works fine in terms of message delivery and delay but fails in reducing network overhead and number of message replicas. Computation of CFV takes more time as this process may also causes high message transmission delay. Also a black hole node may manipulate its CFV value to gain benefits from network. The scheme was only applicable with spray and wait routing. In Spray and wait routing two phases are there spray phase and wait phase. In spray phase messages are replicated and in wait phase sender node waits for a reply after sending replicated messages. When sender got reply in any one of the direction then node transmits messages only in that particular direction. In this scheme sender node depends on a neighbour node remembering a neighbour node which might be a black hole node and it could perform harmful action in network.

To overcome these above mentioned drawbacks of cooperative mechanism we propose a mechanism in which a grade is assigned to each node based on their packet delivery ratio. Also set a minimum threshold value i.e. 40%. It means that nodes having less then 40% drop rate are black hole nodes. This mechanism may reduce overhead ratio, increases delivery ratio and reduces drop rate.

VI. CONCLUSION

In this paper cooperation based mechanism has been discussed to contrast black hole nodes in DTN. A CFV value of each node is calculated by checking node history separately. Node history is stored in nodes buffers. This history provides information related to data transmission of each node means how many packets node created, number of packets it received, number of packets dropped and number of sent packets. After computation of CFV value of each node then this value is compared with a predefined value and distinguish normal nodes and black hole nodes. From normal nodes black hole nodes are nodes that drop maximum packets or deliver wrong messages in

network. Based on CFV mechanism it is intended to propose and enhanced mechanism to contrast black hole attack with less overhead ratio and high delivery ratio meanwhile also drop rate should be low.

REFERENCES

[1] Yinghui Guo, Sebastian Schildt and Lars Wolf , "Detecting Blackhole and Greyhole Attacks in Vehicular Delay Tolerant Networks" , IEEE, 2013.
[2] K.Devi and P.Damodharan, "Detecting Misbehavior Routing And Attacks In Disruption Tolerant Network Using Itrm", *International Conference on Current Trends in Engineering and Technology, ICCTET'13,* 2013.
[3] Gianluca Dini and Angelica Lo Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network". Ad Hoc Netw. (2012).
[4] Jaydip Sen, Sripad Koilakonda and Arijit Ukil, "A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks".
[5] Adnan AHMED, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb and Abdul Wahid KHAN, "A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks", 2014.
[6] Amit Kumar Gupta, Indrajit Bhattacharya, Jyotsna Kumar Mandal, "A Co-Operative Approach to Thwart Selfish AndBlack-Hole Attacks in DTN for Post Disaster Scenario, 978-1-4799-4272-5/14 $31.00 © 2014 IEEE doi 10.1109/EAIT.2014.24, pp. 113-118.
[7] Y. Ren, M.C.Chuah, J.Yang, and Y.Chen, "Muton: Detecting malicious nodes in disruption-tolerant networks," in WCNC'10, pp. 1-6, 2010.
[8] G. Wu, J. Wang, L. Yao and C. Lin, "A Secure Social-aware Incentive Scheme for Delay Tolerant Networks", *in Proc. of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications,* 2013.
[9] Q. Li; S. Zhu; G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *Infocom, 2010 IEEE Proceedings* , pp.1-9, 14-19, March 2010.
[10] A. Al Hinai, H. Zhang and Y. Chen, "Mitigating Black-hole Attacks in Delay Tolerant Networks", *In Proc. of the 13th International Conference on Parallel and Distributed Computing, Applications and Technologies,* 2012.
[11] F. Li, J. Wu, A. Srinivasan. "Thwarting Blackhole Attacks in Distruption-Tolerant Networks using Encounter Tickets", *In Proc. of the IEEE Infocom,* 2009.
[12] Gianluca Dini and Angelica Lo Duca, "Towards a Reputation-based Routing Protocol to Contrast Blackholes in a Delay Tolerant Network" Ad Hoc Netw. (2012),pp:1-12.
[13] Abderrahmane Baadache and AliBelmehdi, "Fighting against packet dropping misbehavior in multi-hop wireless ad hoc networks", *Journal of Network and Computer Applications 35* (2012), pp. 1130–1139.
[14] Heta Changela and Amit Lathigara, Algorithm to Detect and Overcome the Black Hole Attack in MANETs, *International Journal of Computer Applications (0975 – 8887) Vol. 124 (8),* 2015, pp. 22-25.
[15] Soufiene Djahel, Farid Na¨ıt-abdesselam, and Zonghua Zhang , "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges", *IEEE Communications Surveys & Tutorials, Vol. 13 (4*), 2011, pp. 658-672.
[16] Garima Gupta , Preeti Nagrath, Sandhya Aneja and Neelima Gupta, "Reference based approach to Mitigate Blackhole Attacks in Delay Tolerant Networks", ACM, 2012, pp. 85-88.
[17] Atul Sharma, "A Credit Based Routing Mechanism to Contrast Selfish Nodes in Delay Tolerant Networks", *IEEE International Conference on Parallel, Distributed and Grid Computing,* 978-1-4799-7683-6/14/$31.00©2014, and pp: 295-300.
[18] El Ouadrhiri, A., El Kamili, M., Raiss El Fenni, M., Omari, L., "New Forwarding Strategy for PROPHET Routing in DTNs", NETYS 2013, LNCS 7853, pp. 300–305. Springer, Heidelberg (2013).
[19] Zhiting, L., Xiufang, J., "Universal scheme improving probabilistic routing in delay-tolerant networks", Computer Communications 36(2013) 849-860.
[20] A.Al Hinai, H. Zhang and Y. Chen, "Mitigating Black-hole Attacks in Delay Tolerant Networks", *In Proc. of the 13th International Conference on Parallel and Distributed Computing, Applications and Technologies,* 2012.
[21] G. Wu, J. Wang, L. Yao and C. Lin, "A Secure Social-aware Incentive Scheme for Delay Tolerant Networks", *in Proc. of the 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications,* 2013.
[22] J. Miao, O. Hasan, S. B. Mokhtar, L. Brunie, and K. Yim, "An Analysis of Strategies for Preventing Selfish Behavior in Mobile Delay Tolerant Networks", *In Proc. of the 6th IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS '12,* Washington DC, USA, pp. 208-215, 2012.
[23] A. Martin-Campillo, J. Crowcroft, E. Yoneki, R. Marti, "Evaluating opportunistic networks in disaster scenarios", *Journal of Network and Computer Applications 36,* pp. 870-880, 2013.