Sunil Kumar al. International Journal of Recent Research Aspects ISSN: 2349-7688, Vol. 5, Issue 1, March 2018, pp. 325-329

Detecting and Avoiding of Selfish Nodes in Delay Tolerant Networks (DTNs)

Sunil Kumar

Maharaja Agrasen University, Baddi (Distt. Solan), Himachal Pradesh

Abstract- **Sparse Mobile Ad hoc Networks are a class of Mobile Ad Hoc Networks (MANETs) in which the population of nodes is sparse, and the interactions between the nodes in the network are infrequent. This leads to the problem of how to route a packet from one node to another and message delivery must be delay-tolerant, in such a network. This problem becomes more complex, when a node attempts to utilize the network resources for its own benefits, but reluctant to spend its resources for others in such Delay Tolerant Networks (DTNs). This shows how a node behaves as selfish and non-cooperative. This selfish behaviour of any node within the network may lead to destruction of basic operation of network because cooperative behaviour of nodes is the root of MANETs. Hence it is important to detect and isolate such nodes from the normal functioning of the network. In this paper, an algorithm is proposed to detect such selfish nodes in Delay Tolerant Networks (DTNs) based on their selfish degree.**

Keywords— MANETs, DTNs, Selfish Nodes, PRoPHET etc.

I. Introduction

A Mobile Ad hoc NETwork (MANET) is a wireless local area network model composed of a significant number of mobile nodes without a fixed infrastructure (i.e., base stations or access points) [1]. Due to the limited transmission capability of mobile nodes in the MANET, the intermediate nodes are used for forwarding the packets for other nodes in multi-hop fashion [2]. Thus, each node in MANETs acts as router to forward the packets for other nodes. The basic operation of MANETs relies on the cooperation of individual nodes that constitutes the network. However, distributed and cooperative nature of routing algorithms in MANETs makes them highly vulnerable to various security attacks [3, 4].

Delay Tolerant Network (DTN) is a class of Mobile Ad hoc Networks (MANETs) [5] where instantaneous end-to-end paths are difficult or impossible to establish. The routing protocols must take into account the message switching approach (hop-by-hop routing with "store and forward" approach) where data is incrementally moved and stored throughout the network in hopes to reach its destination. Therefore, the routing protocols of DTNs are not same as traditional wireless routing protocols. DTNs are partitioned wireless ad hoc networks with sporadic connectivity, and the probability of isolated nodes are increased [6]. Therefore the communication opportunities Delay Tolerant Networks (DTNs) are usually short and sporadic [7]. Since, nodes in MANETs have the resource constraints such as storage capacity, CPU processing power, link capacity during communication, and limited battery power. They have to spend their resources in forwarding the packets for others. Especially, the data transmission in terms of power consumption is the most expensive service in MANETs.

In [8], Al-Karaki and Kamal proved that the energy spent by a mobile node to transmit a bit over 10 or 100 m distance is same to perform thousands to millions of arithmetic operations. Buttyan and Hubaux [9] showed that when the average number of hops from a source to a destination is around 5 then almost 80% of the transmission energy will be devoted in packet forwarding. As a result, a node may act as selfish (non-cooperative) by refraining from forwarding the packets for others in order to save its precious resources [10, 11]. Over the course of time, the non-cooperative activities of such selfish nodes may significantly decrease the performance of the network, especially in Delay Tolerant Networks. Therefore, in this paper, an algorithm is presented to detect such selfish nodes in Delay Tolerant Networks (DTNs) based on their selfish degree.

Section 2 summarises the related work. In Section 3, the relevant elements of the proposed algorithm are described. In Section 4, the experimental design and simulation results are presented. Finally, Section 5 concludes the proposed approach and provides the directions to future work..

II. Related work

As per authors [12,13,14], the attackers or malicious nodes in Delay Tolerant Networks (DTNs) perform different types of malicious activities in order to violate the core security principles, i.e. confidentiality, integrity and availability (CIA). Just as in traditional networks, malicious nodes within a DTN may attempt to delay or destroy data in transit to its destination. Such attacks include dropping data, flooding the network with extra messages, corrupting routing tables, and counterfeiting network acknowledgments. In [15], authors carried out the study to find out the impacts of blackhole and packet flooding attacks in a post disaster communication network using DTN. In [16], authors suggested a variety of attack strategies with their complex results, and they also introduced attack modalities with a defense for the most powerful. William D. Ivancic [17], work in the field DTN security and proposed a title "Security Analysis of DTN Architecture and Bundle Protocol Specification for Space-Based Networks" in this paper they provides a security analysis of DTN RFCs and proposed security related internet drafts with a focus specially on space-based communication networks. They focused the bundle security (each layer security) while group communication involve in order to increases the privacy and reliability of the DTN

communication. In [18], authors proposed a technique to detect black hole attack in Delay Tolerant Networks (DTNs). S.Karthika et. al [19] has a title proposed an integrated approach of Trust and Fuzzy logic based for Delay Tolerant Networks to secure the communication.

Xin Jiang and Xiang-Yu Bai [20] gave the emphasize on the selfishness problem of nodes in the DTN network. In [21], authors classified the different types of selfish behavior. They classified the existing techniques for preventing selfish behavior into three categories: barter-based, credit-based and reputation-based, and also carried out experimentally study of these techniques. In [22] , authors considered four types of nodes based on cooperation probability and selfish detection algorithm is applied to different routers: Spray and Wait Router Epidemic Router, Direct Delivery Router, Prophet Router, and MaxProp Router. They compared the results in terms of packet delivery ratio and number of selfish nodes detected. They concluded that Spray and Wait router shows highest packet delivery ratio and highest number of selfish nodes detected as compared to other routers. A co-operative scheme [23] is presented to reduce the destructive effects of malicious and selfish nodes in the network. In this paper, authors used a cooperative approach where the malicious behavior of a node is examined at the time of sending messages to that node by inquiring other neighbouring nodes about the past performances of that node. By the cooperation of other neighbouring nodes, a combined faith value (CFV) is computed to judge the behaviour of the node.

III. Proposed Algorithm

Selfish degree of any node is defined as the willingness of the node to cooperate in the routing activities of a node. The range of selfish degree of a node varies from 0 to α (threshold value) which is computed on the basis of the numbers of routing packets drop by the node in the network over a duration of time.

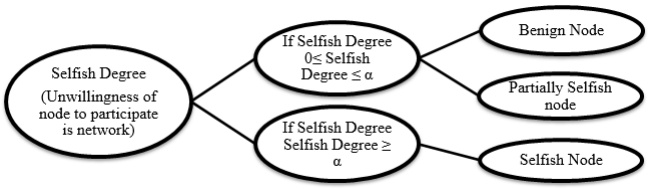

Figure 1: Benign and Selfish nodes classification based on selfish degree.

It may also be defined as a number that represents unwillingness of node to accept or forward the routing messages within the network. If node has selfish degree 0 then it is considered as normal node but if it has degree equals or more than α, then it is considered as fully selfish node. The node may be considered as partially selfish if selfish degree of a node is greater than 0 and less than α. The main aim of this algorithm is to detect selfish nodes in the network on the basis of its selfish degree which is basically their unwillingness to participate normal functioning of the network as shown in figure 1. The selfish degree varies from from 0 to α (threshold value).

Algorithm 1 : Detect selfish nodes ( )

Step 1: Parameter Initializations

N: Total Number of Nodes in the networks

S: Sender

R: Receiver

Sd: Selfish Degree of a node

Step2: For $(i = 1;\ i \le N;\ i++)$ // Monitor the Non-Cooperative activities of every node//

{

If Node cooperates in normal functioning of the network ( ) = true;

No Change in Node Sd;

Else Node cooperates in normal functioning of the network ( )= false;

$Sd++$;

}

Step3: For $(i = 1;\ i \le N;\ i++)$ // Assign the status to the nodes based on their Selfish Degree//

{

If $Sd == 0$

Node is considered Benign Node;

Else If $Sd \ge \alpha$

Node is fully Selfish Node;

Else

Node is Partially Selfish Node;

}

Algorithm Detect selfish nodes ( ) is designed to detect selfish nodes from networks. In this algorithm, the selfish nodes are detected based on their selfish degree. The selfish degree simply represents unwillingness of node to accept or forward the routing messages within network. As stated in the algorithm, if a node cooperates in normal functioning of the network i.e. if the value node cooperates in normal functioning of the network () function is true then there is no change in the selfish degree of the node. Otherwise if this function gives a false value then there is increment in the selfish degree of the node. On the basis of node's selfish degree, the respective node is considered fully selfish or partially selfish node. In proposed algorithm, the range of selfish degree is varied from 0 to α (threshold value). The selfish degree 0 means no selfish node while selfish degree α means fully selfish node, and if the selfish degree of a node lies between 0 to α (threshold value) then respective node is considered as partially selfish node. On the confirmation and detection of fully selfish node, the respective node is isolated from the normal functioning of the network.

IV. Network Simulation and Performance Evaluation

In this paper, ONE (Opportunistic Network Environment) [24] simulator is used. ONE is a Java based simulator

specially targeted for research in Delay Tolerant Networks (DTNs). The simulation environment in ONE simulator basically combines movement modelling, routing simulation, visualization and reporting in one program. Movement modelling can be done either on-demand using the integrated movement models or the movement data can be imported from an external source. The active routing modules included in ONE simulator are [24]: First Contact, Direct Delivery, Spray and Wait (normal and binary), Epidemic, PRoPHET and MaxProp. The core part of ONE simulator is an agent-based discrete event simulator. ONE simulator can be run on Linux, Windows, or any other platform that supports Java.

TABLE 1: SIMULATION PARAMETERS

Parameters	Values
Simulator	ONE(Opportunistic Network Environment)
Movement Model	Shortest Path Map based
Routing	PRoPHET
TTL	300 min
Simulation Area	4500*3400
No. of Nodes	150

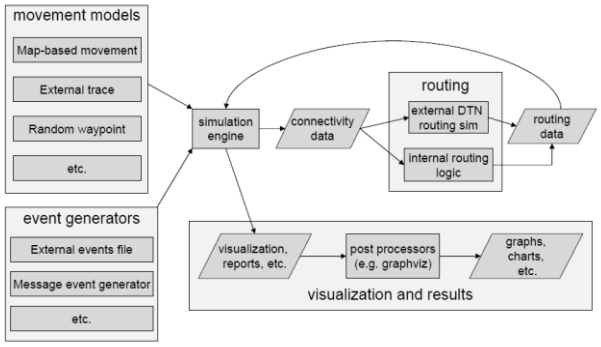

Figure 2: Overview of the ONE simulation environment [24].

Probabilistic Routing Protocol (PRoPHET) [25] uses an algorithm that attempts to exploits the non- randomness of real world encounters by maintaining a set of probabilities for successful delivery of packets to destination in DTN. Further, the performance of the proposed algorithm is analysed with PRoPHET routing protocol in the presence of selfish nodes in terms of the following metrics:

- Packet Delivery Ratio (PDR): PDR is defined as the ratio of total number of data packets successfully delivered to the destination node to the number of data packets originated by the source node throughout the simulation..
- Throughput: It is defined as the amount of data transferred from source to destination per unit of time.
- Average End to End Delay (AEED): AEED is referred as an average transmission delay experienced by data packets from source node to destination node.

Packet Delivery Ratio (PDR)

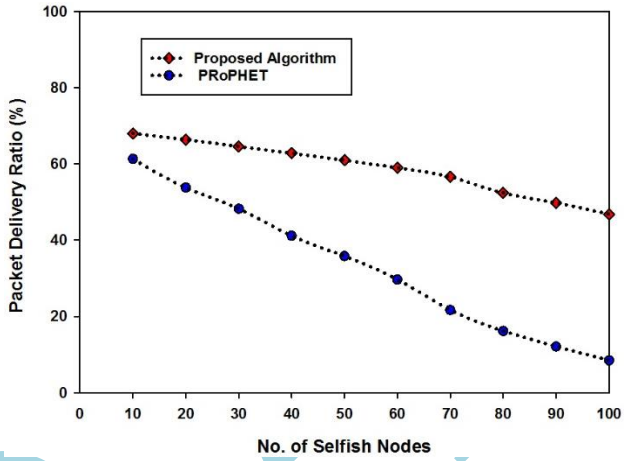

Figure 3: Packet Delivery Ratio vs. No. of Selfish Nodes.

As can be seen from figure 3, in the presence of selfish nodes the proposed algorithm protocol has a higher packet delivery ratio as compared to PRoPHET routing protocol during the simulation run because the proposed approach detects the selfish nodes in the network and isolate them from normal functioning of the network.

Throughput

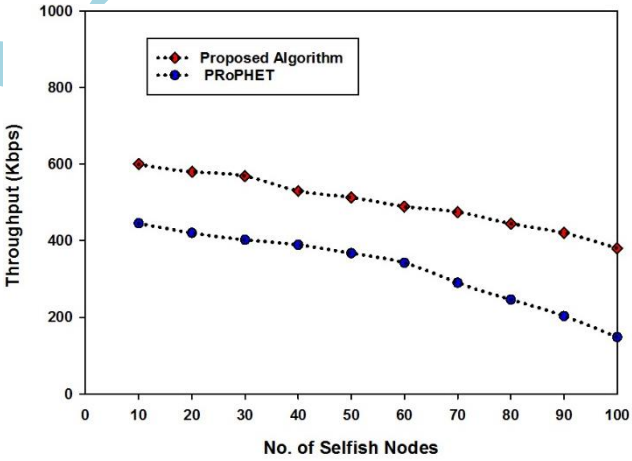

Figure 4: Throughput vs. No. of Selfish Nodes.

As shown in figure 4, the throughput of the network decreases very sharply with the increase in percentage of selfish nodes in PRoPHET routing protocol in the network. However, the proposed algorithm shows better performance as compared to PRoPHET routing protocol in the presence of selfish nodes.

Average End-to-End Delay (AEED)

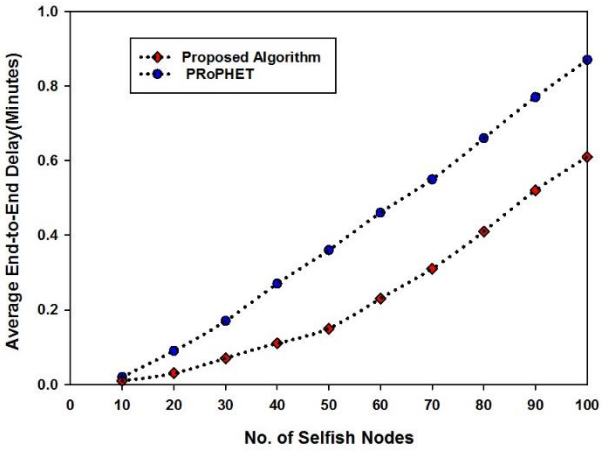

Figure 5: Average End-to-End Delay vs. No. of Selfish Nodes.

As shown in figure 5, the proposed algorithm has less average end-to-end delay as compared to PRoPHET routing protocol increase in percentage of selfish nodes in the network.

V. Conclusion

In this paper, an algorithm is presented to detect such selfish nodes in Delay Tolerant Networks (DTNs) based on their selfish degree. Simulation results clearly show that in the presence of selfish nodes, the packet delivery rate, throughput and average end to end delay of network with PRoPHET routing protocol is affected at a high rate, and finally performance of the network is reduced. The simulation results for proposed detection algorithm also show its effectiveness packet delivery rate, throughput and average end to end delay of network.

REFERENCES

1. J. Hoebeke, I. Moerman, B. Dhoedt and P. Demeester, “An overview of mobile ad hoc networks: applications and challenges”, Journal-Communications Network, vol. 3, no. 3, pp. 60-66, 2004.
2. I. Chlamtac, M. Conti and J.J. Liu,“Mobile ad hoc networking: imperatives and challenges”, Ad hoc networks, vol. 1, no.1, pp.13-64,2003
3. K. Nadkarni and A. Mishra, "Intrusion detection in MANETs-the second wall of defense" Industrial Electronics Society, 2003, IECON'03, The 29th Annual Conference of the IEEE, vol. 2, pp. 1235-1238, 2003.
4. S. Kumar and K. Dutta, “Securing Mobile Ad Hoc Networks: Challenges and Solutions”, International Journal of Handheld Computing Research (IJHCR), vol.7, no.1, pp.26-76, 2016.
5. R. S. Mangrulkar and M. Atique, “Routing protocol for Delay Tolerant Network: A survey and comparison,” In Proceeding of 2010 International Conference On Communication Control And Computing Technologies, pp. 210-215, 2010.
6. M. R. Schurgot, C. Comaniciu, and K. Jaffres-Runser, “Beyond traditional DTN routing: social networks for opportunistic communication,” IEEE Communications Magazine, vol. 50, no. 7, pp. 155–162, 2012.
7. J. Papaj and L. Dobos, “Cooperation between Trust and Routing Mechanisms for Relay Node Selection in Hybrid MANET-DTN,” Mobile Information Systems, vol. 2016, pp. 1–18, 2016.
8. J. N. Al-Karaki and A. E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication, vol. 11, no. 6, pp. 6–28, Dec 2004.
9. L. Buttyan and J. P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks”, ACM/Kluwer Mobile Networks and Applications, vol 8, no.5, 2003.
10. S. Kumar, K. Dutta, and G. Sharma, “A detailed survey on selfish node detection techniques for mobile ad hoc networks,” In Proceeding of Fourth IEEE International conference on parallel, distributed and grid computing. IEEE, pp 122–127 , 2016.
11. S. Kumar, and K. Dutta, "Intrusion detection in mobile ad hoc networks: techniques systems and future challenges", Security and Communication Networks, vol. 9, no. 14, pp. 2484-2556, 2016.
12. D Sarawagya Singh, K Elayaraja, "Survey Of Misbehaviors Of Node And Routing Attack In Delay Tolerant Network", International Journal of Science Engineering and Technology Research (IJSETR), vol. 4, no. 2, February 2015.
13. S Ardra, A. Viswanathan, "A Survey On Detection And Mitigation Of Misbehavior In Disruption Tolerant Networks", IRACST - International Journal of Computer Networks and Wireless Communications (IJCNWC), vol. 2, no. 6, December 2012.
14. F. Li, A. Srinivasan, and J. Wu, “Thwarting Blackhole Attacks in Distruption Tolerant Networks Using Encounter Tickets,” IEEE Procceding INFOCOM, 2009.
15. P. Asuquo, H. Cruickshank, Z. Sun, and G. Chandrasekaran, “Analysis of DoS Attacks in Delay Tolerant Networks for Emergency Evacuation,” 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015.
16. J. Burgess, G. D. Bissias, M. D. Corner, and B. N. Levine, “Surviving attacks on disruption-tolerant networks without authentication,” In Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing - MobiHoc 07, 2007.
17. W. D. Ivancic, “Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks,” 2010 IEEE Aerospace Conference, 2010.
18. R. Sharma and D.V.Gupta, “Blackhole Detection and Prevention Strategies in DTN,” International Journal of Engineering and Computer Science, Vol. 5 No. 8, pp. 17386-17391, August 2016.
19. S. Karthika, and N. Vanitha, “Secure Routing Protocol in Delay Tolerant Networks Using Fuzzy Logic Algorithm”, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 4, Issue 5, May 2015,
20. X. Jiang and X.-Y. Bai, “A survey on incentive mechanism of delay tolerant networks,” In Proceedings

of 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), pp.191,197, 17-19 Dec. 2013.

21. 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," 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2012.
22. R. Kadam and M. Bangare, "Analysis of Delay Tolerant Network Routers by Implementing Selfish Node Detection Algorithm with an Incentive Strategy," International Journal of Science and Research (IJSR), Vol. 5 No. 7, pp. 701-703 , July 2016.
23. A. K. Gupta, I. Bhattacharya, P. S. Banerjee, and J. K. Mandal, "A Co-operative Approach to Thwart Selfish and Black-Hole Attacks in DTN for Post Disaster Scenario," 2014 Fourth International Conference of Emerging Applications of Information Technology, 2014.
24. A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," In Proceedings of the Second International ICST Conference on Simulation Tools and Techniques, 2009.
25. H. A. Nguyen, S. Giordano, A. Puiatti, "Probabilistic Routing Protocol for Intermittently Connected Mobile Ad Hoc Networks (PROPICMAN)", In Proceeding of IEEE WoWMoM/AOC, June 2007.

