Impact of Selfish Node Concentration 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. In this paper, the main objective is to thoroughly capture and analysis the impact of selfish nodes on Delay Tolerant Networks (DTNs) performance using PRoPHET routing protocol with increasing the selfish nodes in the network. The impact of selfish nodes on the performance of DTNs is evaluated using ONE (Opportunistic Network Environment) simulator and results of simulations are presented using three important metrics, which are throughput, packet delivery ratio, and average end-to-end delay. The results of simulations show that the performance of network decreases seriously with increasing the selfish nodes in the network.**

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, the main objective is to thoroughly capture and analysis the impact of selfish nodes on Delay Tolerant Networks (DTNs) performance using PRoPHET routing protocol with increasing the selfish nodes in the network. The impact of selfish nodes on the performance of DTNs is evaluated using ONE (Opportunistic Network Environment) simulator and results of simulations are presented using three important metrics, which are throughput, packet delivery ratio, and average end-to-end delay. The results of simulations show that the performance of network decreases seriously with increasing the selfish nodes in the network.

Section 2 discusses the different types of selfish behavior that a node can exhibit. Section 3 summarizes the related work. In Section 4, the experimental design and simulation results are presented. Finally, Section 5 discusses conclusion and future work.

II. Selfish Node

Any node in MANETs may act selfishly, which means getting the utmost profits from the network resources, but reluctant to spend its resources for others. In [12, 13], authors stated that a selfish node can exhibit its selfish behaviour in the following ways:

a) TYPE 1 –These types of selfish nodes forward the routing packets, but, don't forward the data messages intentionally for other nodes in the network.

b) TYPE 2 –These selfish nodes neither forward data packets nor forward the routing packets, or modify the Route Request and Reply packets by changing the TTL value to smallest possible value.

c) TYPE 3 –These selfish nodes change their behaviour dynamically by dropping packets based on its residual energy.

d) TYPE 4 –These selfish nodes forward the routing messages with a delay near the upper limit of timeout change in order to avoid being the active route member for others.

If intermediate nodes act as non-cooperative nodes (selfish nodes) and refuse to forward packets, the communication beyond radio range is not possible. Over the course of time, the selfish activities of such nodes may leads to significantly decrease in the performance of the network.

III. Related Work

As per authors [14,15,16], 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 [17], 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 [18], 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 [19] proposed Bundle Protocol Specification for Space-Based Networks. They provides a security analysis of DTN RFCs and also 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 [20], authors proposed a technique to detect black hole attack in Delay Tolerant Networks (DTNs). S. Karthika et. al [21] proposed an integrated approach of Trust and Fuzzy logic based for Delay Tolerant Networks to secure the communication.

Xin Jiang and Xiang-Yu Bai [22] gave the main emphasize on the selfishness problem of nodes in the DTN network. In [23], 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 [24], 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 [25] 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 behaviour 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.

IV. Network Simulation and Performance Evaluation

In this paper, ONE (Opportunistic Network Environment) [26] simulator is used. ONE is a Java based simulator specially targeted for research in Delay Tolerant Networks (DTNs).

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

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.

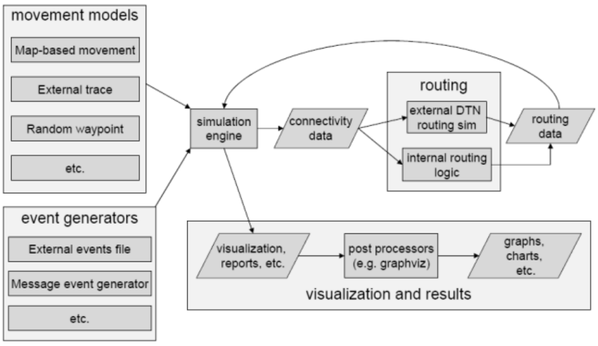


Figure 1: Overview of the ONE simulation environment [26].

The active routing modules included in ONE simulator are [26]: 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.

Probabilistic Routing Protocol (PRoPHET) [27] 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 PRoPHET routing protocol is analysed in terms of the following metrics with increasing the selfish nodes in the network:

- 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)

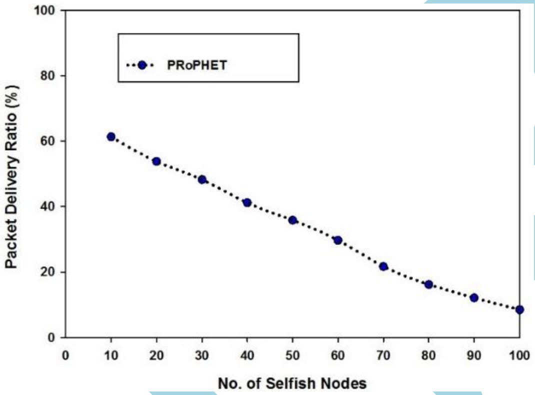


Figure 2: Packet Delivery Ratio vs. No. of Selfish Nodes.

The packet delivery ratio for PRoPHET routing protocol decreases very sharply with increasing the selfish nodes in the network as shown in figure 2. This is due to the non-cooperative activities of selfish nodes in the network, especially in data forwarding and routing processes.

Throughput

As shown in figure 3, the throughput for PRoPHET routing protocol in the network decreases with increasing with increasing the selfish nodes in the network. This is due to selfish nodes discard the packets intentionally rather than forwarding them and effecting overall throughput.

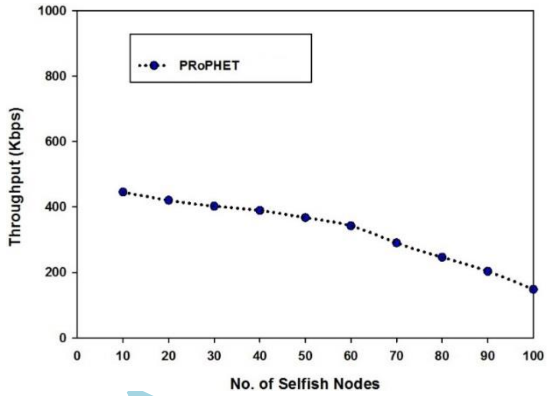
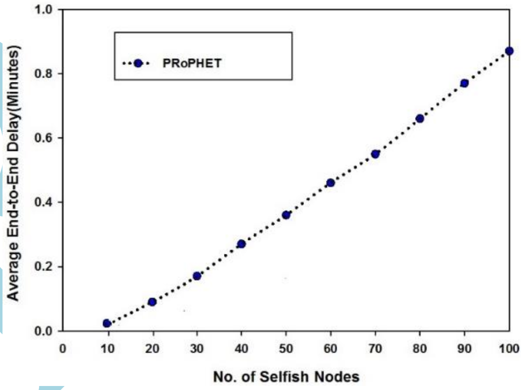


Figure 3: Throughput vs. No. of Selfish Nodes.

Average End-to-End Delay (AEED)



.

Figure 4: Average End-to-End Delay vs. No. of Selfish Nodes.

It is obvious from figure 4 that the Average End to End Delay for PRoPHET routing protocol increases with increasing the selfish nodes in the network. This is due to selfish nodes either discard the packets intentionally for other nodes in the network or avoid themselves to become active member of the route.

V. Conclusion

In this paper, the impact of selfish nodes on Delay Tolerant Networks (DTNs) performance using PRoPHET routing protocol is discussed ONE (Opportunistic Network Environment) simulator. The results of simulations are presented using three important metrics, which are throughput, packet delivery ratio, and average end-to-end delay. The results of simulations clearly show that the performance of network decreases seriously with increasing the selfish nodes in the network. The future proposal will focus on investigating the defense methods against such non-cooperative activities of selfish nodes.

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. S. Subramaniyan, W. Johnson and K. Subramaniyan, "A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique", EURASIP Journal on Wireless Communications and Networking, vol. 2014, no. 1, 2014.
13. J. Sengathir and R. Manoharan, "Exponential reliability coefficient based reputation mechanism for isolating selfish nodes in MANETs" ,Egyptian Informatics Journal, vol. 16, no. 2, pp.231-24, 2015
14. 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.
15. 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.
16. F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Distruption Tolerant Networks Using Encounter Tickets," IEEE Procceding INFOCOM, 2009.
17. 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.
18. 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.
19. W. D. Ivancic, "Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks," 2010 IEEE Aerospace Conference, 2010.
20. 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.
21. 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,
22. 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.
23. 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.
24. 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.
25. 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.
26. 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.
27. 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.