Evaluating the Performance Characteristics of the Epidemic and Spray-and-Wait Routing Protocols during a Black Hole Attack on an Opportunistic Network

Oliver Mitchell
psyom1@nottingham.ac.uk

School of Computer Science
University of Nottingham

October 25th, 2018

Contents

1 Introduction

The aim of this project is to evaluate the performance characteristics of two different opportunistic routing protocols within a real world scenario, simulated by the Opportunistic Network Simulator (ONE). In the chosen scenario, malicious nodes engaging in black hole denial-of-service attacks are positioned within a network topology that represents the city of Helsinki and its transport network, including cars, buses and trams.

To begin, this paper will give a brief overview of opportunistic networks, the 2 protocols, and the DoS attack in question. Then, the functionality of the ONE simulator will be described and the model of the scenario explained in detail, including its implementation. Using this model, simulations will be run and the results of their performances critically evaluated. A conclusion will then be drawn based on these results, summarising the pros and cons of opportunistic networks and their use in the observed scenario. Finally, the paper closes with a wider discussion of the usefulness of opportunistic networks in related real world use-cases.

2 Background

In recent years, a growing number of devices have been utilizing mobile networking technology in less traditional environments, ranging from the GPS tracking of wildlife over huge distances [5], to the proposed establishment of an "Interplanetary Internet", capable of transmitting data lightyears in distance [6]. These non-static networks are decentralised and wireless, consisting of constantly mobile nodes, ranging from those with predictable mobility, such as transport systems, (e.g. buses and trams) to those with stochastic mobility, such as military/tactical networks. In all of these new environments, communication coverage is pervasive and essential for day-to-day operations. However, it's impossible to treat them like traditional networks with pre-determined communication paths due to their constant reconfiguration and non-guaranteed connectivity. As a result, computer networks deployed in such environments face new challenges such as large delays, intermittent communication links, and heterogeneous nodes with differing operating systems and network protocols.

2.1 Mobile Ad-Hoc Networks (MANETs)

A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile devices, with no fixed infrastructure, connected by wireless links. An important characteristic of a MANET is each node's ability to move independently in any direction, forcing the network to reconfigure itself frequently. Each node acts as a client, server, and router simultaneously in order to transport packets from source to destination, thus nodes communicate with each other in a peer-to-peer fashion [8]. There are several important properties that limit the effectiveness of MANETs [7]:

- Security is difficult to achieve because wireless links are vulnerable, the topology is dynamically changing, and there is no certification authority [9].
- The use of wireless links results in a lower capacity than wired counterparts [7].
- Nodes are mobile devices which rely on exhaustible battery power. Therefore saving energy is an important system design aspect [7].

MANETs assume high connectivity and established routes for transmitting data between nodes in a multi-hop fashion. As a result, the routing process in MANETs requires the discovery of an end-to-end path before data can be transported. However, because the topology is constantly changing in most mobile ad-hoc networks, there may not always be a feasible end-to-end path between source and destination [7]. Resultantly, MANETs perform poorly when connections are intermittent or there are long delays. This problem presents the need for the improved protocols used in opportunistic networks and Delay Tolerant Networks (DTNs).

2.2 Vehicular Ad-Hoc Networks (VANETs)

Vehicular Ad-Hoc Networks (VANETs) are a type of MANET where the network's nodes are represented by vehicles. Though MANETs and VANETs share many characteristics, there are unique challenges exclusive to VANETs that affect their usability, efficiency, and therefore their system design [10]:

- Vehicles have the potential to move at very high speeds which can reduce the length of time available for packet transfer between nodes communicating in proximity to each other [10]. As VANETs also require end-to-end paths to be established before data can be sent, this issue is compounded by the movement of intermediary nodes in multi-hop transmissions. The path may be established before transmission begins, but disrupted before the packet can reach its destination.
- The data transmitted by vehicles may be critical and life-saving, such as road accidents, traffic information, or the location of casualties for ambulances. It is therefore essential that information is received correctly and timely [10].

It is useful to note that the movement of nodes in a VANET can be considered more predictable than coventional ad-hoc networks because vehicles follow set paths such as roads, railway lines, etc.

2.3 Delay/Disruption Tolerant Networks (DTNs)

In environments where disruptions and delays are expected, traditional networking protocols such as TCP [4] are unsuitable because they assume there is an end-to-end connection with low message loss and minimal delay [3]. In decentralised, mobile ad-hoc networks, nodes are constantly moving and there is likely no feasible end-to-end path between source and destination. In order to combat the challenges presented by delays and disruptions, the assumption of an existing end-to-end path from source to destination is dropped. Instead, routing protocols have been developed which utilise a "store-and-forward" approach where data is gradually transported in single hops and stored in different nodes with the desire of eventually reaching its intended destination [3]. Typically, this approach to network architecture is called Delay/Disruption Tolerant Networking (DTN).
The performance of a DTN depends on the routing protocol used in a given scenario. DTN routing protocols can either be replication based (flooding) or forwarding based [11]:

- In a replication based protocol, when one node encounters another it will forward a copy of its message without deleting its own. This means there are multiple copies of the message in the network with aims to increase the probability that a message will eventually reach its destination. However, in this approach a large amount of resources are used, particularly buffer space. Once the message has been delivered, all existing copies of the message are made redundant but still continue to exist, taking up unecessary space [11].
- In a forwarding based protocol, a message can only be stored by a single node at a time. In constrast to a replication based scheme, the node forwarding the message deletes its own copy, making the receiver the sole custodian of the message. Forwarding based protocols tend to use heuristics to evaluate encountered nodes and work out which path is most likely to get the message to its destination the quickest.

2.4 Delay/Disruption Tolerant Network (DTN) Protocols

2.4.1 Epidemic

Epidemic [12][13] is a simple dissemination based routing protocol and is somewhat naïve when compared to other, more advanced protocols. The objective of the epidemic routing protocol is to pass copies of a message to as many nodes as possible in the hope that it eventually reaches its intended destination with minimal delay. Any node that doesn't already have the message will be given a copy and there can exist as many copies of the message as there are nodes in the network. The protocol is called 'epidemic' because this indiscriminate method of dissemination is similar to the way in which an infectious disease can propogate in a community; spreading when people come into contact with each other.

Theoretically, Epidemic can be seen as an optimal routing protocol if the network's resource are unconstrained. However, in a deployed DTN the size of each node's message buffer is finite and because no acknowledgement of receipt is transmitted by the destination node, it is likely that redundant data will still take up unecessary space in the network. Some research has produced extended versions of the epidemic protocol which mitigate this issue, typically by sending an additional message that confirms receipt and orders 'infected' nodes to delete redundant messages [13].

2.4.2 Spray-and-Wait

Spray-and-Wait [14] is a routing protocol that aims to achieve the advantages of Epidemic's high delivery probability but with far less resource utilisation. It achieves this by disseminating a finite quantity of message copies (spraying) with the recipients storing the message until direct contact with the destination node. The maximum number of messages to spray is typically configured by a variable, $\boldsymbol{L}$. There are 2 versions of the spray-and-wait protocol: vanilla and binary. The difference between them is the method used to disseminate the message copies to $\boldsymbol{L}$ different nodes.

- **Vanilla** - transmit one copy of the message to the first $\boldsymbol{L - 1}$ nodes encountered. Each node with 1 copy of the message waits until the destination node comes into direct contact.
- **Binary** - start with $\boldsymbol{L}$ copies and transmit $\boldsymbol{L/2}$ copies to the first node encountered. Both these nodes then transmit $\boldsymbol{n/2}$ copies of the message to any new nodes they encounter that do not have the message, where $\boldsymbol{n}$ is the total number of messages a node currently holds. When a node has 1 copy remaining, it waits until the destination node comes into direct contact.

Binary has an advantage over vanilla because messages are disseminated away from the source at a faster rate [14].

2.5 Opportunistic Networks

2.6 Black Hole Attacks

Black hole attacks (also known as packet dropping attacks)[2][15] are a form of denial of service (DoS) attack where a connected node erroneously advertises itself as an opportunistic next-hop in the route of a packet's transmission. Once the malicious node receives a packet it does not forward it, preventing the message from ever reaching its destination.

Despite their directness, black hole attacks can be difficult to detect; more sophisticated attackers are likely to drop small quantities of packets over specific time periods, rather than dropping all packets ad infinitum. This is harder to detect because some traffic still flows over the network. Additionally, some research has defined "collaborative" black hole attacks [2] where multiple malicious nodes work together to fabricate routing information and disrupt the flow of packets. This paper observes scenarios involving both single and collaborative black hole attacks.

3 ONE Simulator

The ONE (Opportunistic Network Environment) Simulator [16][17] is a DTN simulator developed and maintained by researchers on the SINDTN and CATDTN projects and supported by Nokia Research Center (Finland). Where existing DTN simulators focused on solely on routing simulation, ONE combines DTN routing, mobility modelling, and visualisation into one package [16]. It is a complex tool which is extensible and provides useful modules for the reporting and analysis of simulated network environments.

ONE is useful for comparing, contrasting and analysing the performance of opportunistic networking protocols in different scenarios, making it the ideal tool for this research article. Scenarios (or network models) are comprised of network nodes (hosts) which all possess user-specified networking interfaces, energy sources, buffer-sizes, and computing power. Collections of identical nodes can be defined as groups with default properties, though an individual node's settings can be overwritten if necessary, for example, to ensure a node uses a different routing protocol from the rest of its group. Nodes act autonomously, passing messages to other nodes within their communication range according to their designated routing protocol.

ONE also makes a comprehensive framework for the mobility of nodes available to the user, allowing them to customise the travel speed of individual nodes or groups of nodes, and even import real-world movement traces for nodes to follow. This high fidelity node mobility framework allows users to easily differentiate between different node types (e.g. pedestrians will move slower than cars and follow a different route) and permits the creation of highly accurate scenarios that use real-world data, or hybrid scenarios which combine real traces with user-defined rules.

Creating custom scenarios involves the editing of the ONE simulator's config files.

The ONE Simulator provides a GUI.

The ONE Simulator can be extended.

4 Experiment

Experiment

5 Evaluation

Evaluation

5.1 Epidemic in a Black Hole Attack Scenario

Epidemic

5.2 Spray-and-Wait in a Black Hole Attack Scenario

Spray-and-Wait

6 Conclusion

Conclusion

7 Wider Discussion

Wider Discussion

References

[1] Huang, C., Lan, K., & Tsai, C. (2008). "A Survey of Opportunistic Networks". *22nd International Conference on Advanced Information Networking and Applications - Workshops (aina workshops 2008)*, pp.1672-1677.

[2] Tseng, F.H., Chou, L.D, & Chao H.C. (2011) "A Survey of Black Hole Attacks in Wireless Mobile Ad Hoc Networks" *Human-centric Computing and Information Sciences* **1**(4)

[3] Farrell, S., & Cahill, V. (2006) *Delay- and Disruption-Tolerant Networking*, Artech House, Inc., Norwood, MA.

[4] Postel, J. (1981), "Transmission Control Protocol". RFC 793.

[5] Juang, P., Oki, H., Wang, Y., Martonosi, M., Shiuan Peh, L., & Rubenstein, D. (2002). "Energy-Efficient Computing for Wildlife Tracking: Design Tradeoffs and Early Experiences with ZebraNet". *ACM SIGOPS Operating Systems Review* **36**(5), pp.96–107

[6] Jackson, J. (2005). "The Interplanetary Internet" *IEEE Spectrum.* Available at: https://spectrum.ieee.org/telecom/internet/the-interplanetary-internet [Accessed 24 Oct. 2018].

[7] Giordano, S (2002). "Mobile Ad-Hoc Networks" *Handbook of Wireless Networks and Mobile Computing* pp.325-346

[8] Singh, S., Dutta, S.C., & Singh D.K. (2012). "A Study on Recent Research Trends in MANET" *International Journal of Research and Reviews in Computer Science (IJRRCS) **3**(3), pp.1654-1658*

[9] Djenouri, D., Khelladi, L., & Badache, A.N. (2005). "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks" *IEEE Communications Surveys and Tutorials* **7**(4), pp.2-28

[10] Dahiya, A., & Chauhan, R.K. (2010). "A Comparative Study of MANET and VANET Environment" *Journal of Computing* **2**(7), pp.87-92

[11] Rani, S., & Abhilasha (2015). "Performance Evaluation of various Flooding and Forwarding Protocols based on Delay Tolerant Networks: A Review" *International Journal of Science and Research (IJSR)* **4**(7), pp.1625-1629

[12] Vahdat, A., & Becker, D. (2000). "Epidemic Routing for Partially-Connected Ad Hoc Networks" *Department of Computer Science, Duke University, Durham*

[13] Zhang, X., Neglia, G., Kurose, J., & Towsley, D. (2007) "Performance Modelling of Epidemic Routing" *Computer Networks* **51**(10), pp.2867-2891

[14] Spyropoulos, T., Psounis, K., & Raghavendra, C.S. (2005) "Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks" *Proceedings of the 2005 ACM SIGCOMM Workshop on Delay-Tolerant Networking*, pp.252-259

[15] Zhang, X., Wu, S.F., Fu, Z., & Wu, T.S. (2000) "Malicious Packet Dropping: How It Might Impact the TCP Performance and How We Can Detect It" *Proceedings of the 2000 International Conference on Network Protocols*, pp.263-272

[16] Karänen, A. (2008). "Opportunistic Network Environment Simulator". *Helsinki University of Technology, Department of Communications and Networking*

[17] The ONE (Opportunistic Network Environment Simulator). Available at: https://akeranen.github.io/the-one/ [Accessed 4th Dec. 2018]