# Evaluating the Performance Characteristics of the Epidemic and Spray-and-Wait Routing Protocols During DOS Attacks

Oliver Mitchell
psyom1@nottingham.ac.uk

School of Computer Science
University of Nottingham

October 25th, 2018

## Contents

**1 Introduction 2**

**2 Background 2**
2.1 Opportunistic Networks . . . . . 2
2.2 Mobile Ad-Hoc Networks (MANETs) . . . . . 2
2.3 Vehicular Ad-Hoc Networks (VANETs) . . . . . 2
2.4 Delay Tolerant Networks (DTNs) . . . . . 2
2.5 Delay Tolerant Network Protocols . . . . . 2
2.5.1 Epidemic . . . . . 2
2.5.2 Spray-and-Wait . . . . . 3
2.6 DOS Attacks . . . . . 3
2.6.1 Black Hole Attack . . . . . 3
2.6.2 Flood Attack . . . . . 3

**3 ONE Simulator 3**

**4 Experiment 3**

**5 Evaluation 3**
5.1 Scenario 1 - Black Hole Attack . . . . . 3
5.1.1 Epidemic . . . . . 3
5.1.2 Spray-and-Wait . . . . . 3
5.2 Scenario 2 - Flood Attack . . . . . 3
5.2.1 Epidemic . . . . . 3
5.2.2 Spray-and-Wait . . . . . 3

**6 Conclusion 4**

**7 Wider Discussion 4**

**References 4**

# 1 Introduction

In recent years, a growing number of devices have been utilizing networking technology in increasingly less traditional environments. These non internet-like networks can range from those with predictable mobility, such as transport systems, (e.g. buses and trams) to stochastically mobile networks, 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 the non-static nature of each node. As a result, computer networking in such environments faces new challenges such as large delays, intermittent communication links, and heterogeneous nodes with differing operating systems and network protocols.

The aim of this project is to evaluate the performance characteristics of two different opportunistic routing protocols within real world scenarios, simulated by the Opportunistic Network Simulator (ONE). In the chosen scenarios, malicious nodes engaging in various DoS (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 attacks in question. Then, the functionality of the ONE Simulator will be described and the model of each scenario explained in detail, including their implementations. Using these models, 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 scenarios. Finally, the paper closes with a wider discussion of the usefulness of opportunistic networks in related real-world scenarios.

# 2 Background

Background

## 2.1 Opportunistic Networks

Opportunistic Networks

## 2.2 Mobile Ad-Hoc Networks (MANETs)

Mobile Ad-Hoc Networks (MANETs)

## 2.3 Vehicular Ad-Hoc Networks (VANETs)

Vehicular Ad-Hoc Networks (VANETs)

## 2.4 Delay Tolerant Networks (DTNs)

Delay Tolerant Networks (DTNs)

## 2.5 Delay Tolerant Network Protocols

Delay Tolerant Network Protocols

### 2.5.1 Epidemic

Epidemic

#### 2.5.2 Spray-and-Wait

Spray-and-Wait

### 2.6 DOS Attacks

DOS Attacks

#### 2.6.1 Black Hole Attack

Black Hole Attack

#### 2.6.2 Flood Attack

Flood Attack

## 3 ONE Simulator

ONE Simulator

## 4 Experiment

Experiment

## 5 Evaluation

Evaluation

### 5.1 Scenario 1 - Black Hole Attack

Scenario 1 - Black Hole Attack

#### 5.1.1 Epidemic

Epidemic

#### 5.1.2 Spray-and-Wait

Spray-and-Wait

### 5.2 Scenario 2 - Flood Attack

Flood Attack

#### 5.2.1 Epidemic

Epidemic

#### 5.2.2 Spray-and-Wait

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] Jhaveri, R., Patel, S., & Jinwala, D. (2012). "DoS Attacks in Mobile Ad-Hoc Networks: A Survey". *2012 Second International Conference on Advanced Computing & Communication Technologies*, pp.535-541.

[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.