Electronic Communications of the EASST
Volume 080 (2021)

Conference on Networked Systems 2021
(NetSys 2021)

On the Resilience of Opportunistic Networks against DoS Attacks

S. Afzali, A. Udugama, A. Förster and M. Fischer

4 pages

Guest Editors: Andreas Blenk, Mathias Fischer, Stefan Fischer, Horst Hellbrueck, Oliver Hohlfeld, Andreas Kassler, Koojana Kuladinithi, Winfried Lamersdorf, Olaf Landsiedel, Andreas Timm-Giel, Alexey Vinel
ECEASST Home Page: http://www.easst.org/eceasst/ ISSN 1863-2122

On the Resilience of Opportunistic Networks against DoS Attacks

S. Afzali[1], **A. Udugama**[1], **A. Förster**[1] **and M. Fischer**[2]

[1] University of Bremen, Germany
[2] University of Hamburg, Germany

Abstract: Opportunistic Networks (OppNets) enable contact-based networking and service provisioning when no infrastructure exists, e.g., in disaster areas. In such sensitive scenarios, maintaining their availability is important, but most existing work on OppNets mainly assume fully cooperative and thus not malicious nodes. In this paper, we study the impact of different flavors of low-intensity Denial of Service (DoS) attacks on OppNets, which are hard to detect and to counter. Our results indicate that low-rate DoS and black hole attacks as a special case of DoS, seem to have a huge impact on the packet delivery ratio and the delivery delay of an OppNet.

Keywords: Opportunistic Networks, Attacker Models, Security, OPS, OMNeT++

1 Introduction

Opportunistic Networks (OppNets) are networks used to communicate in environments where end-to-end paths and networking infrastructure are non-existent. Applications that use OppNets have to be delay tolerant and nodes exploit any available communication opportunity to exchange information with other nodes using direct communication. Communication in the aftermath of disasters, for remote or unconnected villages, or for offloading saturated networks are some of the scenarios where OppNets can play an important role. An integral and critical part of an OppNets node is the forwarding mechanism employed to exchange data between nodes. There are a number of forwarding protocols developed to efficiently exchange data [KTUF19]. However, these protocols assume well behaving nodes only. However, there are many types of attacks that can inflict damage on a network and thus also on OppNets. OppNets might be seriously affected by Denial of Service (DoS) and as special case of DoS also by blackhole attacks [ADA16].

The main contribution of this paper, is an evaluation of the impact of low-rate DoS and black hole attacks on OppNets, so that efficient countermeasures can be developed in the future. Our results indicate that both attack types can significantly decrease the packet delivery ratio of OppNets. The remainder of this paper is structured as follows: Section 2 briefly summarizes related work. Section 3 describes our methodology and Section 4 our evaluation results. Section 5 concludes the paper.

2 Related Work

A survey of the previous work on evaluating attacks on OppNets shows that almost all focus on individual attack models and improvements to protocols rather than on a collective look on the severity of the problem[ADA16]. There exist also some work on analysis of attack models for some specific protocols like MaxProp [CCC10]. In this work, we look at the impact of low-rate DoS and black hole attacks and quantify to which extent they can degrade the network operation.

In a **low-rate DoS attack**, the attacker injects apparently valid packets into the network to deplete the network bandwidth and forwarding resources of other nodes for legitimate users. A special case of DoS is a **blackhole attack**, in which malicious nodes do not cooperate with the rest of the network and thus only request and receive messages, without ever forwarding them.

3 Methodology

Dos Attacks - In this paper we mainly focus on low-rate DoS attacks and black hole attacks. Both types of attacks are hard to detect and hard to counter in an OppNet setting. In a low-rate DoS attack, a malicious node will send garbage packets to other nodes to consume resources and to impede the forwarding of legitimate content. In a black hole attack, a malicious node will receive packets, but will never forward them. Hence, such a node is consuming transmission resources of other nodes without contributing the own resources for spreading content.
Simulation - The evaluation of the effects of DoS attacks on OppNets are performed using the OMNeT++ network simulator together with the OppNets framework *OPS* [UFDK19]. In this work, OPS has been extended with two attacker models described in Section 2. Unlike traditional networks, OppNets have a specific set of **evaluation metrics** that highlight their performance: the *Delivery Ratio*, the network wide ratio of packets successfully delivered over the total expected packets, and *Average Delay*, the network wide average of the time taken for a packet to reach a destination. These two metrics are independent of each other and typically used to benchmark OppNets.
Simulation Setup - The simulated OppNet consists of 50 nodes, including attackers and genuine nodes. Each simulation run is set to 5 days. Data (packets) by genuine nodes are injected into the network every 900 seconds, with a payload of 10 KB each. The forwarding of packets are limited by a maximum of 30 hops. Nodes are configured to have infinite caches. The wireless connectivity is configured to be Bluetooth LE like with a range of 30 meters and a bandwidth of 100 Kbps. Mobility of nodes is modelled using the SWIM Mobility model. The mobility area is 1,500 meters by 1,500 meters. Epidemic routing [VB00] is used to disseminate data, probably the best one and used protocol for OppNets. This experimental setup is quite standard for OppNets and sufficient to show the severity of DoS attacks [KTUF19].

The *attack configuration* includes the attacker model, the attack frequency, and the number of attackers explored. Unless otherwise stated, attackers inject malicious data every 90 seconds.

4 Results

In this section we summarize our results on black hole and low-rate DoS attacks on OppNets.
Black holes - Figure 1 plots the delivery ratio (left) and the delivery delay (right) in 95% confidence intervals in dependence on a varying number of black hole nodes and by keeping the overall number of nodes constant at 50 (red graph) and in dependence on a varying number of legitimate nodes without malicious nodes as baseline (blue graph). With an increasing number of black holes, the delivery of data decreases and the delivery delay increases. Even at this rather low attack intensity it can be seen that the effect is significant. The results also indicate that a black hole node does not correspond to a decreased density of the network. While 25 black hole nodes in a setting with in total 50 nodes decrease the delivery ratio to under 50%, the delivery

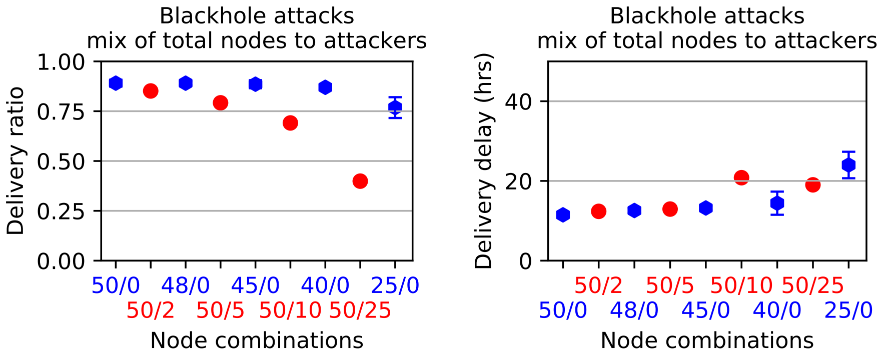

Figure 1: Delivery ratio (left) and delivery delay (right) for a varying number of malicious nodes carrying out black hole attacks. *50/2* refers to 50 total nodes and two of them are attackers.

ratio stays at around 75% for a comparable setting with 25 legitimate nodes only and thus lower density. This is due to the fact that attackers still occupy networking resources, forcing legitimate nodes to waste their contact times on black hole nodes that do not forward their content.

Low-rate DoS - Figure 2 shows the delivery ratio and delivery delay of OppNets during DoS attacks for varying number of attacking nodes and attack frequencies and for a setting with malicious nodes (red graphs) and a setting without (red graphs). The graphs indicate that with an increasing number of attackers (top row) and increasing attack intensity (bottom row), the performance deteriorates quickly. Already five attacking nodes are sufficient to decrease the delivery ratio from close to 100% to around 60%, while the average delivery delay nearly doubles at the same time. At the same time, delivery ratio and delay stay nearly constant from 50 to 45 legitimate nodes without any attackers.

5 Conclusion

In this work, we have evaluated the performance of OppNets in the presence of two relevant attacker models. We have explored DoS attacks and Blackhole attacks via simulations. Our results are very interesting and show potential new directions for security-aware protocols in OppNets. Blackhole and DoS attacks severely impact the performance of the network, even at low-intensity attacks which are very hard to detect.

In the future, we plan to explore systematically further OppNets relevant attack models.At the same time, we will focus on developing counter-measures for them. Furthermore, we will explore also the impact of DoS and Blackhole attacks with data dissemination protocols other than Epidemic.

References

[ADA16] M. Alajeely, R. Doss, A. Ahmad. Security and Trust in Opportunistic Networks – A Survey. *IETE Technical Review* 33(3):256–268, May 2016.

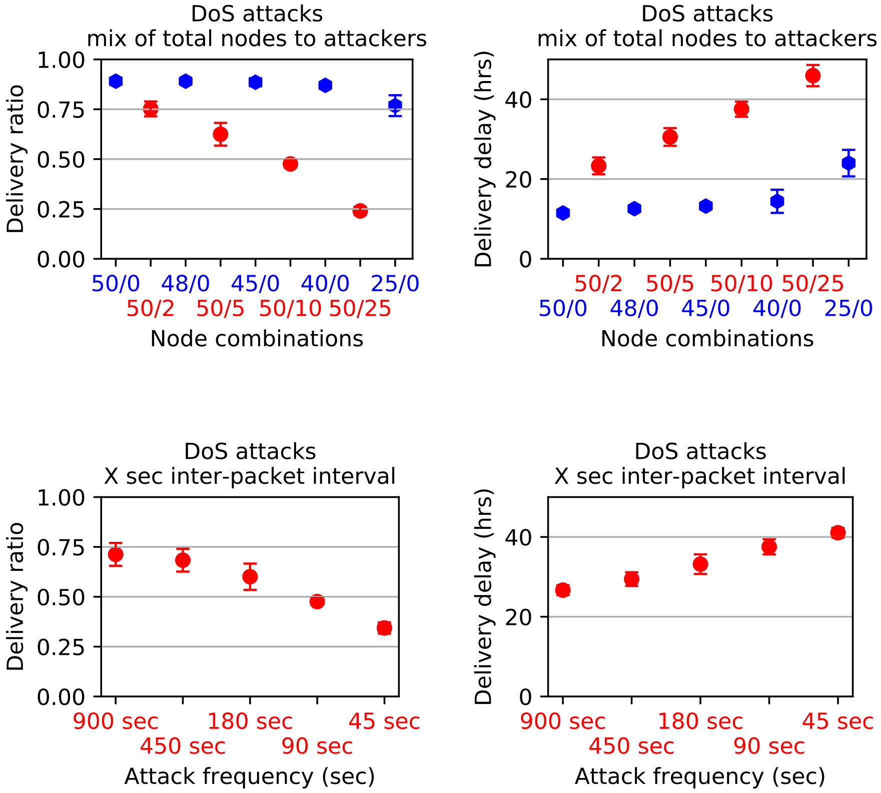

Figure 2: Effect of DoS attacks by varying attackers (top row) and attack intervals (bottom row). In the top row *50/2* refers to 50 nodes from which two are attackers (95% confidence intervals). In the bottom row, the network uses a *50/10* node combination for each attack frequency.

[CCC10] F. C. Choo, M. C. Chan, E. Chang. Robustness of DTN against routing attacks. In *2010 Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010)*. Pp. 1–10. 2010.

[KTUF19] V. Kuppusamy, U. M. Thanthrige, A. Udugama, A. Förster. Evaluating forwarding protocols in opportunistic networks: Trends, advances, challenges and best practices. *Future Internet* 11(5):113, 2019.

[UFDK19] A. Udugama, A. Förster, J. Dede, V. Kuppusamy. Simulating Opportunistic Networks with OMNeT++. In Virdis and Kirsche (eds.), *Recent Advances in Network Simulation: The OMNeT++ Environment and its Ecosystem*. Pp. 425–449. 2019.

[VB00] A. Vahdat, D. Becker. Epidemic routing for partially-connected ad hoc networks. Technical report, 2000.