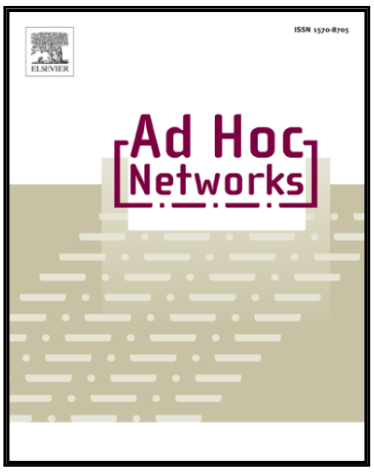

Modeling and Performance Evaluation of Security Attacks on Opportunistic Routing Protocols for Multihop Wireless Networks

Mahmood Salehi, Azzedine Boukerche, Amir Darehshoorzadeh

PII: S1570-8705(16)30174-3
DOI: 10.1016/j.adhoc.2016.07.004
Reference: ADHOC 1417

To appear in: *Ad Hoc Networks*

Received date: 15 December 2015
Revised date: 10 May 2016
Accepted date: 8 July 2016

Please cite this article as: Mahmood Salehi, Azzedine Boukerche, Amir Darehshoorzadeh, Modeling and Performance Evaluation of Security Attacks on Opportunistic Routing Protocols for Multihop Wireless Networks, *Ad Hoc Networks* (2016), doi: 10.1016/j.adhoc.2016.07.004

Modeling and Performance Evaluation of Security Attacks on Opportunistic Routing Protocols for Multihop Wireless Networks

Mahmood Salehi, Azzedine Boukerche, Amir Darehshoorzadeh

School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Ontario, Canada

Abstract

In wireless networks, Opportunistic Routing (OR) protocols are designed to route data packets towards their destination with greater reliability than traditional routing schemes. In addition to reliability, nodes' trustworthiness and willingness to cooperate can also play a significant role in the delivery of packets to their final destinations. More specifically, nodes in the network may be compromised, experience software or hardware failures, or behave maliciously for various reasons. Therefore, it would be beneficial to model the behavior of malicious or uncooperative nodes and study their effects in a wireless network that employs OR for communications. In this paper, the behavior of malicious nodes in a wireless mesh network that utilizes unicast opportunistic routing protocols is modeled using Discrete Time Markov Chain (DTMC). Afterwards, using the proposed model, we introduce a novel approach for the calculation of packet drop ratio, through which the negative effects of uncooperative nodes can be calculated. Furthermore, a customized version of a black-hole attack is introduced as an example of malicious behavior in OR protocols; we apply this routing attack to several well-known OR protocols, with the additional use of network simulation as well as through the proposed analytical technique. Finally, a comprehensive set of performance evaluation scenarios is designed and applied, with

*Corresponding author

Email addresses: msalehi@uottawa.ca (Mahmood Salehi), boukerch@site.uottawa.ca (Azzedine Boukerche), adarehsh@uottawa.ca (Amir Darehshoorzadeh)