

Accepted Manuscript

Security-oriented opportunistic data forwarding in Mobile Social Networks

Dapeng Wu, Feng Zhang, Honggang Wang, Ruyan Wang

PII: S0167-739X(17)30120-6

DOI: <http://dx.doi.org/10.1016/j.future.2017.07.028>

Reference: FUTURE 3558

To appear in: *Future Generation Computer Systems*

Received date: 20 January 2017

Revised date: 3 May 2017

Accepted date: 10 July 2017

Please cite this article as: D. Wu, F. Zhang, H. Wang, R. Wang, Security-oriented opportunistic data forwarding in Mobile Social Networks, *Future Generation Computer Systems* (2017), <http://dx.doi.org/10.1016/j.future.2017.07.028>

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.



Security-Oriented Opportunistic Data Forwarding in Mobile Social Networks

Dapeng Wu^a, Feng Zhang^a, Honggang Wang^{b,*}, Ruyan Wang^a

^a*Department of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*

^b*University of Massachusetts Dartmouth.*

Abstract

In recent years, Mobile Social Networks (MSNs) have been arising a growing interest in both scientific and industrial fields for its potential value. The effective data transmission of MSNs is generally achieved through opportunistic forwarding and node collaboration. However, malicious nodes may illegally intercept and drop the data packets which should be forwarded. Therefore, it is very challenging to detect these malicious nodes. In this paper, we proposed a new Resisting On-Off Attack Data Forwarding Mechanism (OADM) for MSNs to detect the on-off attack, which not only prevents malicious nodes from intercepting data packets, but also exploits the node collaboration to forward data packets. Our major contribution includes: (1) Exploiting Hidden Markov Model (HMM) model to learn node behaviors for the evaluation of attacking probabilities and node states; (2) Effective relay node selection based the estimation of node capability. Results show the proposed OADM can effectively identify the attacking behavior and collaborating states of nodes and significantly improve the data delivery rate of MSNs.

Keywords: Mobile Social Networks; Malicious Behaviour Detection; Trust and Reputation Management; Opportunistic Forwarding

*Corresponding author

Email address: Email: hwang1@umassd.edu (Honggang Wang)

Download English Version:

<https://daneshyari.com/en/article/6872965>

Download Persian Version:

<https://daneshyari.com/article/6872965>

[Daneshyari.com](https://daneshyari.com)