Accepted Manuscript

A Sybil attack detection scheme for a forest wildfire monitoring application

Mian Ahmad Jan, Priyadarsi Nanda, Xiangjian He, Ren Ping Liu

PII: S0167-739X(16)30152-2
DOI: http://dx.doi.org/10.1016/j.future.2016.05.034
Reference: FUTURE 3058

To appear in: *Future Generation Computer Systems*

Received date: 1 September 2015
Revised date: 24 May 2016
Accepted date: 25 May 2016

Please cite this article as: M.A. Jan, P. Nanda, X. He, R.P. Liu, A Sybil attack detection scheme for a forest wildfire monitoring application, *Future Generation Computer Systems* (2016), http://dx.doi.org/10.1016/j.future.2016.05.034

A Sybil Attack Detection Scheme for a Forest Wildfire Monitoring Application

Mian Ahmad Jan[a,b], Priyadarsi Nanda[a,*], Xiangjian He[a,*], Ren Ping Liu[b]

[a] *School of Computing and Communications, University of Technology, Sydney, Australia*
[b] *Wireless and Networking Laboratory, CSIRO, Sydney, Australia*

Abstract

Wireless Sensor Networks (WSNs) have experienced phenomenal growth over the past decade. They are typically deployed in human-inaccessible terrains to monitor and collect time-critical and delay-sensitive events. There have been several studies on the use of WSN in different applications. All such studies have mainly focused on Quality of Service (QoS) parameters such as delay, loss, jitter etc. of the sensed data. Security provisioning is also an important and challenging task lacking in all previous studies. In this paper, we propose a Sybil attack detection scheme for a cluster-based hierarchical network mainly deployed to monitor forest wildfire. We propose a two-tier detection scheme. Initially, Sybil nodes and their forged identities are detected by high-energy nodes. However, if one or more identities of a Sybil node sneak through the detection process, they are ultimately detected by the two base stations. After Sybil attack detection, an optimal percentage of cluster heads are elected and each one is informed using nomination packets. Each nomination packet contains the identity of an elected cluster head and an end user's specific query for data collection within a cluster. These queries are user-centric, on-demand and adaptive to an end user requirement. The undetected identities of Sybil nodes reside in one or more clusters. Their goal is to transmit high false-negative alerts to an end user for diverting attention to those geographical regions which are less vulnerable to

*Corresponding author
Email addresses: Priyadarsi.Nanda@uts.edu.au (Priyadarsi Nanda), Xiangjian.He@uts.edu.au (Xiangjian He)