Journal of Network and Computer Applications 34 (2011) 1380–1397

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks

Y. Challal [a,*], A. Ouadjaout [b], N. Lasla [b], M. Bagaa [b], A. Hadjidj [a]

[a] Université de Technologie de Compiègne, Heudiasyc, UMR CNRS 6599, France
[b] Centre d'Etude et de Recherche sur l'Information Scientifique et Technique, Algeria

ARTICLE INFO

Article history:
Received 1 October 2010
Received in revised form
16 February 2011
Accepted 10 March 2011
Available online 16 March 2011

Keywords:
Wireless sensor networks
Security
Multipath routing

ABSTRACT

In wireless sensor networks, reliability is a design goal of a primary concern. To build a comprehensive reliable system, it is essential to consider node failures and intruder attacks as unavoidable phenomena. In this paper, we present a new intrusion-fault tolerant routing scheme offering a high level of reliability through a secure multipath routing construction. Unlike existing intrusion-fault tolerant solutions, our protocol is based on a distributed and in-network verification scheme, which does not require any referring to the base station. Furthermore, it employs a new multipath selection scheme seeking to enhance the tolerance of the network and conserve the energy of sensors. Extensive analysis and simulations using TinyOS showed that our approach improves many important performance metrics such as: the mean time to failure of the network, detection overhead of some security attacks, energy consumption, and resilience.

1. Introduction

Wireless Sensor Networks (WSN) is a promising technology for gathering real time information in order to monitor a specific area. Their low cost and ease of deployment make them an attractive solution for a plethora of applications in various fields, such as military tracking, fire monitoring, *etc*. They consist of short range sensing devices that collaborate to carry out monitoring measurements to the end users. Sensor nodes are characterized by some intrinsic properties representing important design factors, such as energy constraints, limited computation and storage capacities, *etc*. In addition, many applications require deploying sensors in harsh environments and in large quantities, making very difficult the manual control and the individual monitoring of sensors. Consequently, failures of nodes become *an inevitable phenomenon* which can reduce dramatically the overall network lifetime and make the communication infrastructure unusable.

Some solutions addressing the network lifetime problem are based on *energy-aware routing mechanisms*, which construct paths using some energy metrics (Al-Karaki and Kamal, 2004). The concept behind this family of protocols is to postpone nodes failure as far as possible, but this method is not enough satisfactory since the operation of the whole network is not guaranteed after the occurrence of these failures that are *inevitable*. More elaborate solutions consider node failure as *a normal property of the network* and enhance the network lifetime by providing fault tolerant mechanisms that guarantee normal operation of the network in presence of failures. Major tolerant solutions for WSN and MANET are based on the multipath routing paradigm, which provides each sensor with alternative paths. Different kinds of multipath schemes have been proposed, offering different levels of reliability and fault tolerance (Ganesan et al., 2001; Lou and Kwon, 2006). Among these schemes, building node-disjoint paths has been considered as the most reliable one. Due to the absence of common sensors between node-disjoint paths, a link disconnection will cause at most *a single path to fail* for any sensor in the network. This can contribute greatly in prolonging the network lifetime since failures do not cause a significant impact into the routing view of sensors.

In real deployments, security becomes another important issue (Ouadjaout et al., 2009; Karlof and Wagner, 2003; Djenouri et al., 2005). In presence of malicious nodes, providing sensors with alternative paths is not sufficient to ensure a reliable system. Thus, it is vital to merge intrusion-tolerant solutions with fault tolerant ones in order to obtain a dependable routing layer able to work in any situation.

In the literature, existing *intrusion-fault tolerant* solutions suffer from many problems and shortcomings. Secure protocols trying to find node-disjoint paths consume an important amount of control messages and thus are not adequate to large scale WSN. On the other hand, secure protocols trying to provide a better

* Corresponding author. Tel.: +33 344234429; fax: +33 344234477.
E-mail addresses: ychallal@hds.utc.fr (Y. Challal), aouadjaout@mail.cerist.dz (A. Ouadjaout), nlasla@mail.cerist.dz (N. Lasla), bagaa@mail.cerist.dz (M. Bagaa), hadjidj@utc.fr (A. Hadjidj).

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.03.022