Journal of Network and Computer Applications ■ (■■■■) ■■■–■■■

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Review

# Survey of secure multipath routing protocols for WSNs

Shazana Md Zin [a,b,*], Nor Badrul Anuar [a], Miss Laiha Mat Kiah [a], Ismail Ahmedy [a]

[a] Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya (UM), Kuala Lumpur 50603, Malaysia

[b] Department of Web Technology, Faculty of Computer Science and Information Technology, University of Tun Hussein Onn Malaysia (UTHM), Johor 86400, Malaysia

ARTICLE INFO

*Article history:*
Received 10 September 2014
Received in revised form
6 April 2015
Accepted 28 April 2015

*Keywords:*
Wireless
Sensor
Networks
Routing
Security
Multipath

ABSTRACT

In sensing data to the base station, wireless sensor networks (WSNs) face some security challenges since such networks impose resource constraints that need to be addressed by the routing mechanism. This paper surveys, explores, and informs researchers regarding the landscape of multipath routing by providing the motivation behind multipath routing deployment. Subsequently, this paper analyzes the security requirements and common attacks in wireless sensor networks. We provide a classification of secure multipath routing protocols on the basis of nature of defense against the WSN attacks. According to the classification, we investigate the existing secure multipath routing protocols within the WSN domain by discussing their strengths, limitations, and efficiency analysis. A comparative study of the suggested classification is presented based upon the multipath technique, additional security infrastructure, security requirements, corresponding attacks, and efficiency in pursuit of effective secure routing in wireless sensor networks.





**Contents**



* Corresponding author at: Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya (UM), Kuala Lumpur 50603 Malaysia. Tel.: +60 197771712.
*E-mail address:* shazanamdzin@gmail.com (S.M. Zin).

http://dx.doi.org/10.1016/j.jnca.2015.04.018
1084-8045/

## 1. Introduction

In recent years, there has been a huge interest in wireless sensor networks (WSNs) (Rawat et al., 2014). With the advancement in technology, many real applications have been deployed and new application areas have rapidly emerged. The sensor networks are composed of numerous numbers of resource constrained sensor nodes depending on the application, with a few base stations acting as a gateway to the outside network, such as the Internet. Wireless sensor networks have a wide range of applications such as military (Pathan et al., 2006), environmental (Sann and Minn, 2011), and other commercial applications. For instance, the WSN technology can be used to detect the position of incoming attacks in military applications. Moreover, sensor networks can be greatly beneficial for the environment to locate forest fires (Hefeeda and Bagheri, 2007) or to observe animal habits such as ant colonies (Alrajeh et al., 2013a). In healthcare applications (Al Ameen et al., 2010), the nodes are responsible for collecting patients' physiological data and recording their periodic medical assessments. For commercial domain, wireless sensor networks can be deployed for indoor surveillance (Barati et al., 2008) and temperature regulation (Baghyalakshmi et al., 2011) in offices.

Unlike wired networks, routing in WSNs poses more challenges due to the unique characteristics of sensor nodes, such as them being prone to failures due to harsh deployment environments (Jing et al., 2013). Moreover, with the absence of fixed infrastructure, such nodes have to be autonomous and self-organizing within the network area (Lin et al., 2012b). All nodes in a sensor network communicate with each other via a wireless basis, which results to topology changes. Therefore, various attacks can leads to many security problems. For instance, the adversary has the ability to compromise a sensor node, eavesdrop on data transmission, inject false messages, and waste network resources (Yick et al., 2008). Hence, security provisioning for such networks is crucial to route data from source to the destination (Yun et al., 2008). However, there are constraints in incorporating security into a wireless sensor network (WSN) such as limitations in energy, computation, processing, memory, and communication capabilities (Brandl et al., 2009). Therefore, designing a secure protocol requires consideration of such limitations and achieving acceptable performance levels to meet the needs of specific applications. Since security remains a fundamental factor in data communication (Abduvaliyev et al., 2013), many routing protocols have been proposed, such as routing using the multipath mechanism.

The multipath routing technique is widely used to prolong the network lifespan (Nasser and Chen, 2007a) and be responsible for Quality-of-Service (QoS) provisioning (Huang and Fang, 2008) in wireless sensor network applications. Instead of single path, the data are routed through two or more paths, and therefore the multipath mechanism is considered to be more fault tolerant than the conventional single path approach (Alrajeh et al., 2013a). Multipath routing protects data security in WSNs against attacks by reducing the chance of a packet being modified or dropped by a malicious sensor node (Kohno et al., 2012). Moreover, lightweight security mechanism can be adapted to the multipath routing technique to further enhance the security of transmission by mitigating the impact of network attacks in WSNs (Khalil et al., 2010).

As discussed earlier, security provisioning for data communication is challenging in wireless sensor networks. Surveys by (Ehsan and Hamdaoui, 2011; Stavrou and Pitsillides, 2010) show that secure routing is an open issue for WSNs which motivates us to make an effort in this domain. This paper reviews the state-of-the-art for secure multipath routing in WSNs. We discuss the motivation behind the development of multipath routing, security requirements, and attacks on WSN. Besides providing readers with a landscape of multipath routing in WSN, the main purpose of this work is to focus on the needs of security mechanism support in multipath routing, discuss the efficiency of secure multipath approaches, as well as classifying the secure multipath routing on the basis of the nature of defense in responding to network attacks on WSNs. Further, we critically analyze the existing works in this research area. Also, we provide related figures associated with each protocol discussed in this survey. Moreover, the proposed matrix based upon the classification is presented in terms of the multipath technique, security mechanism support, security requirements, corresponding attacks, and efficiency with respect to secure multipath routing protocols in WSNs.

The remainder of the paper is structured as follows. Section 2 presents related work. Section 3 deals with the landscape of multipath routing in WSNs. In Section 4 and Section 5, the security requirements and common attacks on WSNs are discussed, respectively. Section 6 discusses the security mechanism support, efficiency analysis in multipath routing, proposes a classification for secure multipath routing, and analyses the selected protocols based upon the classification. Section 7 summarizes the discussions. Finally, Section 8 provides conclusions derived from this survey. Table 1 shows the list of acronyms used in the paper.

## 2. Related work

The different requirements from various applications reflect the different performance focuses in routing protocol development (Al-Obaisat and Braun, 2007). Thus, many routing protocols have been proposed based upon the application motivations. Moreover, due to the importance of routing protocols, there is a set of literature reviewing the routing techniques of WSNs from various perspectives. Most of the surveys in the literature have focused on reviewing the different routing schemes for WSNs without considering security (Akkaya and Younis, 2005; Raghunandan and Lakshmi, 2011; Yick et al., 2008). Additionally, there are some researchers focused on a survey of security issues who identify relevant open problems for future



Please cite this article as: Zin SM, et al. Survey of secure multipath routing protocols for WSNs. Journal of Network and Computer Applications (2015), http://dx.doi.org/10.1016/j.jnca.2015.04.018