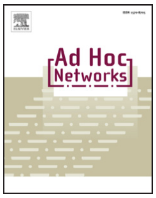
Ad Hoc Networks 36 (2016) 296–307

Contents lists available at ScienceDirect

Ad Hoc Networks

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



Maximum lifetime dependable barrier-coverage in wireless sensor networks[☆]

Donghyun Kim[a,b,*], Hyunbum Kim[c], Deying Li[d], Sung-Sik Kwon[b],
Alade O. Tokuta[b], Jorge A. Cobb[e]

[a] Division of Algorithms and Technologies for Networks Analysis, Faculty of Information Technology, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[b] Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, United States
[c] Department of Computer Science, University of North Carolina at Wilmington, Wilmington, NC 28403, United States
[d] School of Information, Renmin University of China, Beijing 100872, PR China
[e] Department of Computer Science, The University of Texas at Dallas, Richardson, TX 75080, United States

ARTICLE INFO

Article history:
Received 24 November 2014
Revised 3 July 2015
Accepted 6 August 2015
Available online 12 August 2015

Keywords:
Barrier coverage
Wireless sensor network
Maximum lifetime scheduling

ABSTRACT

In a wireless sensor network, a subset of sensor nodes provides a barrier-coverage over an area of interest if the sensor nodes are dividing the area into two regions such that any object moving from one region to another is guaranteed to be detected by a sensor node. Recently, Kumar et al. introduced scheduling algorithms for the maximum lifetime barrier-coverage problem. The algorithms achieved the optimal lifetime by identifying a collection of disjoint subsets of nodes such that each subset in the collection can provide barrier-coverage over the area, and by activating each subset in turn. This introduces a new security problem of these scheduling algorithms called barrier-breach. We show there could be a way to penetrate the area protected by barrier-covers when one barrier-cover is replaced by another. To deal with this issue, we propose three different remedies for the algorithms. In addition, we compare the performance of the three approaches against an upper bound via extensive simulation and make a discussion on the results.

1. Introduction

Wireless sensor network (WSN) is regarded as a decent network technology for a wide range of important applications such as battlefield surveillance, intrusion detection, environmental monitoring, etc. A WSN is composed of a large number of sensor nodes. Each sensor node is equipped with a sensing device, a computing unit, a wireless transceiver and a limited energy source such as a battery. A sensor node can monitor specific phenomenon using the embedded sensing device and forward the data toward a base station [10,11]. In the literature, the coverage provided by a WSN is largely classified into two categories: full-coverage and partial-coverage. A WSN is supporting full-coverage over a target area only if any event happening in the area at any moment is guaranteed to be detected by the WSN [1,3,12–15]. In contrast, a WSN providing partial-coverage may miss some event in an area of interest [2,16–18].

In the literature, a subset of sensor nodes provides barrier-coverage over an area of interest if the sensor nodes are dividing the area into two regions such that any object moving from one region to anther is guaranteed to be detected by a sensor node. As a result, barrier-coverage can be considered as a special case of partial-coverage. There are many

---

[☆] A part of this paper has been appeared in the Proceedings of the *IEEE Global Communications Conference (GLOBECOM 2012)* [4].

[*] Corresponding author. Tel.: +1 (919) 530– 6567.

E-mail addresses: donghyun.kim@tdt.edu.vn, donghyun.kim@nccu.edu (D. Kim), kimh@uncw.edu (H. Kim), deyingli@ruc.edu.cn (D. Li), skwon@nccu.edu (S.-S. Kwon), atokuta@nccu.edu (A.O. Tokuta), cobb@utdallas.edu (J.A. Cobb).

http://dx.doi.org/10.1016/j.adhoc.2015.08.004
1570-8705/

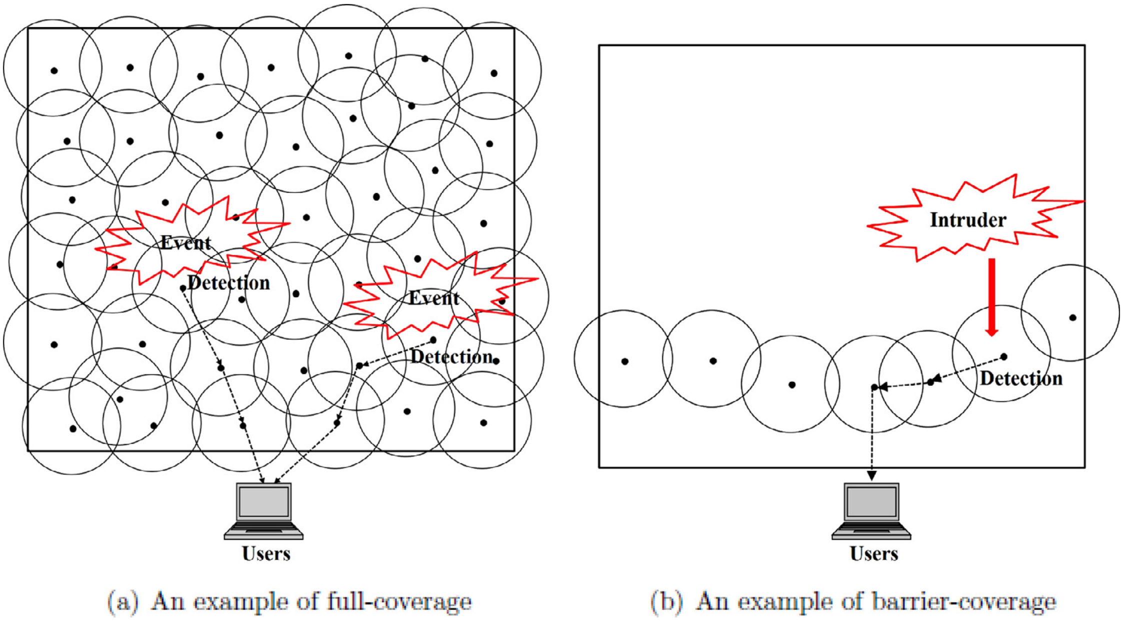


Fig. 1. Illustration of full-coverage and barrier-coverage.

important applications of barrier-coverage such as intrusion detection, and thus it has attracted lots of attentions recently [5–9,19,22–24]. In the rest of this paper, we call a set of sensor nodes providing barrier-coverage over an area simply as a *barrier-cover of wireless sensors*. Fig. 1 illustrates an example of both full-coverage and barrier-coverage.

When it is compared with full-coverage model, barrier-coverage model requires much fewer sensors and thus costs less. Hence, this coverage model has been known to be an attractive approach for various applications such as intrusion detection in which the full-coverage model is somehow excessive. Kumar et al. also introduced the k-barrier-coverage model as a security enhanced model of barrier-coverage. A sensor network provides k-barrier-coverage over an area, where $k \geq 1$ is a given security parameter if any attempt to cross an area covered by the sensor network is guaranteed to be detected by at least k distinct sensors.

In many application scenarios, WSNs are randomly but densely deployed over an area of interest to ensure connectivity. Consequently, it is highly likely that the same target is covered by more than one sensor node simultaneously. Frequently, such a redundancy is appropriately exploited to maximize the lifetime of the sensor networks. For example, if several sensor nodes cover the same target, one can find a sleep-wakeup schedule of the nodes and operate the nodes one by one to maximize the time to cover the target. Clearly, in this way, the total time to cover the target can be extended much longer than the case where all of the sensors are used concurrently. The problem of finding the optimal sleep-wakeup schedule is NP-hard for full-coverage model even if all sensors have equal lifetime. Recently, Kumar et al. [23] have shown that the sleep-wakeup problem for k-barrier-coverage sensor networks is solvable by developing two polynomial time optimal sleep-wakeup algorithms, *Stint* and *Prahari*. The *Stint* considers the case when the remaining battery level of each sensor is same. On the other hand, *Prahari* deliberates on the harder case in which each sensor may have different remaining battery levels.

In this paper, we introduce a new security problem which exists in the sleep-wakeup scheduling algorithms for the maximum lifetime k-barrier-cover of wireless sensors by Kumar et al. To simplify our discussion, we set a security parameter k to 1 and show when a barrier-cover of wireless sensor is replaced with another, the barrier-covers can be useless by one or more locations, namely *barrier-breaches*, which can be exploited by a trespasser to intrude without being detected. Then, we propose three algorithms which can be used to eliminate barrier-breaches from a sleep-wakeup schedule produced by *Stint* and *Prahari*. The first one is applied on the output of the algorithms and the second and third one are applied to the input of the algorithms. At last, we compare the performance of the three approaches against the theoretical upper bound via extensive simulation and analyze the results.

Furthermore, as an extension of [4], we can summarize additional contributions as follows. Firstly, we newly proposed the third algorithm referred as Algorithm 3. Different from previous two algorithms which we considered in [4], the Algorithm 3 focuses on the quality of residual graph by checking the maximum flow value of the residual graph. So, it finally finds the maximum number of node-disjoint paths, which is the maximum number of non-penetrable barriers. Secondly, we implemented Stint and three different algorithms through extensive simulations and various scenarios. Then, we have compared their performances and have shown that the newly proposed Algorithm 3 outperforms other algorithms which we considered in [4]. To show the results, we created all related figure graphs and discussed the results in the new section. Thirdly, we formally defined the introduced problem and enhanced a structure of the paper as well as related studies by considering additional parts and references.