Ad Hoc Networks 9 (2011) 249–264

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Towards robustness and energy efficiency of cut detection in wireless sensor networks ☆

Myounggyu Won *, Stephen M. George, Radu Stoleru

Department of Computer Science and Engineering, Texas A&M University, College Station, TX 77840, United States

ARTICLE INFO

Article history:
Received 8 May 2010
Received in revised form 23 June 2010
Accepted 29 June 2010
Available online 4 July 2010

Keywords:
Wireless sensor networks
Topology control
Network cut detection

ABSTRACT

Reliable, full network connectivity in wireless sensor networks (WSN) is difficult to maintain. Awareness of the state of network connectivity is similarly challenging. Harsh, unattended, low-security environments and resource-constrained nodes exacerbate these problems. An ability to detect connectivity disruptions, also known as cut detection, allows WSN to conserve power and memory while reducing network congestion. We propose ER-CD and LR-CD, protocols that detect cuts while providing energy-efficiency and robustness to attack. Using distributed, cluster-based algorithms, ER-CD recognizes and determines the scope of disrupted connectivity while examining available data for evidence of an attack. For more resource-constrained networks, LR-CD enhances security through the use of a robust outlier detection algorithm. Extensive simulations and a hardware implementation provide experimental validation across a range of network sizes and densities. Results indicate that energy-efficiency can be improved by an order of magnitude in denser networks while malicious nodes are detected at deviations of 1% from expected behavior.

1. Introduction

Wireless sensor networks (WSN), systems composed of numerous sensor nodes with small, low-power, inexpensive radios, have attracted a large amount of research leading to interesting and innovative applications in disaster response [2], military surveillance [3], and medical care [4], among others. However, difficult problems still exist. One of the most challenging problems in WSN is maintaining network connectivity to reliably communicate between peers or deliver data to a specified point, or sink, in an energy-efficient manner. Disrupted connectivity, known as a *cut*, can lead to skewed data, ill-informed decisions and even entire network outages. It can also lead to memory and power exhaustion in disconnected nodes and network congestion in disconnected segments. Such data loss and wasted resources can be avoided when nodes can independently determine if a cut exists.

Cut detection algorithms attempt to recognize and locate cuts. In [5–8], a subset of nodes are given the task of monitoring the connectivity of network. Of particular note is the work by Shrivastava et al. [8] that proposes deterministic and randomized algorithms to detect a linear cut using a set of specially designated entities called sentinel nodes. However, their algorithms are centralized and detect only a linear cut. The state-of-the-art cut detection algorithm, Distributed Source Separation Detection (DSSD) [9], offers a more flexible approach, reliably detecting arbitrarily-shaped cuts, and allowing individual nodes to perform cut detection autonomously by examining the convergence of a positive *state* scalar. However, DSSD suffers from a number of problems. First, the convergence of the state relies heavily on neighboring states. Thus, in a network with dynamically changing topology, convergence is hard to achieve due to the frequently changing neighbor

☆ A preliminary version of this article [1] was presented at the 2009 International Conference on Wireless Algorithms, Systems, and Applications (WASA), 2010. This work was supported in part by NSF Grant CNS-0923203.

* Corresponding author.
E-mail addresses: mgwon@cse.tamu.edu (M. Won), smgeorge@cse.tamu.edu (S.M. George), stoleru@cse.tamu.edu (R. Stoleru).

1570-8705/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.adhoc.2010.06.008

set. Second, DSSD fails to address security, a critical component of sensor deployments in unattended environments. The algorithm can erroneously converge when the network contains a malicious node that injects false state to influence the cut detection decision. Third, DSSD requires a lengthy, iterative convergence process. Since all nodes participate in frequent broadcasts required to achieve convergence, the algorithm is cost-prohibitive with regards to power, especially in denser networks.

In light of these problems, we propose two protocols, *Energy Efficient and Robust Cut Detection* (*ER-CD*) and *Lightweight and Robust Cut Detection Algorithm* (*LR-CD*).

ER-CD is an improved cut detection protocol that offers increased energy efficiency and robustness against masquerade or impersonation attacks. ER-CD divides the network into a grid of location-based clusters. Cluster leaders form a Virtual Grid Network. The cut detection algorithm runs on this high-level network that is significantly less affected by topological changes. As the algorithm executes, the states of leaders converge to some positive value if there is no cut in the network. The speed of convergence is faster thanks to the grid topology of the high level network, since the degree of a leader is typically at most 4. Furthermore, the simple grid topology enables leaders to maintain the global topological information in their adjacency matrices with a small computational cost. By exploiting the adjacency matrix, a leader can exactly compute the next states of its neighbors. Finding any inconsistency above a certain threshold in the states of adjacent leaders potentially indicates a masquerade or impersonation attack. In this attack, a malicious node injects erroneous state into the cut detection process.

LR-CD is a cut detection protocol designed for resource-constrained situations where ER-CD is too heavy. Built on top of the DSSD algorithm, LR-CD incorporates outlier detection, a statistical data analysis technique, to detect a masquerade or impersonation attack. Outlier detection enables the identification of statistically improbable data, a possible indicator of malicious activities, and provides a light-weight mechanism to validate neighbor data.

The contributions of this article are:

- A protocol, ER-CD, that provides reliable cut detection with fast convergence, good energy-efficiency, and robustness against a particular security threat, the masquerade attack.
- A lightweight protocol, LR-CD, that enhances the state of the art cut detection algorithm with robustness against the masquerade attack at low computation and memory cost.
- Extensive simulations that verify and validate performance of the protocols across a variety of network sizes and densities.
- An implementation on Epic wireless sensor motes [10] extending and confirming the simulation results.

This article is organized as follows. Section 2 discusses related work and is followed by the system model and problem formulation in Section 3. Section 4 discusses ER-CD, the proposed algorithm for improving the energy efficiency and robustness against the masquerade attack. LR-CD, a lightweight protocol focused on providing robustness, follows in Section 5. Implementation is addressed in Section 6 which is followed by experimental results in Section 7. Conclusions are presented in Section 8.

2. Related work

The challenges of the network partition monitoring problem have been emphasized in many papers [11–13]. Chong et al. [12] mentions the problem from a security perspective arguing that nodes deployed in a hostile environment must be able to detect tampering. In [13], Cerpa and Estrin stress the importance of the network cut detection problem in their self-configuring topology scheme but left it as a future work. Significant open questions remain in this area.

An early paper by Kleinberg et al. [5] considers the cut detection problem in a wired network. The authors define the (ϵ, k)-cut to be a network separation into $(1-\epsilon)n$ nodes and ϵn nodes when k independent edges are disabled. To detect the (ϵ, k)-cut, they place a set of *agents* D to monitor the connectivity of the network. Each agent periodically communicates with all other agents. Failed connections beyond some threshold are presumed to indicate the presence of a cut. The main result is that the size of the set D must be $O\left(k^3 \frac{1}{\epsilon} \log \frac{1}{\epsilon} + \frac{1}{\epsilon} \log \frac{1}{\delta}\right)$ to successfully detect any kind of (ϵ, k)-cut with probability $1-\delta$. However, in wireless sensor networks, due to their geometric structure, linear or other geometric shaped cuts are more likely than independent k disabled edges. Additionally, the number of agents required for this type of cut detection is very large.

Recently, Shrivastava et al. [8] proposed deterministic and randomized algorithms to detect network separation using a set of sentinel nodes to monitor for linear cuts in a network. The work is, in large part, based on [5]. Specifically, the authors defined the ϵ-cut where at least ϵ fraction of nodes are disconnected by the cut. However, Shrivastava minimized the number of required sentinels by reducing the problem to the linear cut, which is a more natural phenomenon for wireless sensor networks than independent k edge failures, and proved that there exist $O(\frac{1}{\epsilon})$ sentinels for any ϵ-cut with $\epsilon < 1$. This is a relatively small number of sentinels when compared with the result of [5]. The authors proposed a deterministic algorithm to find the minimum number of sentinels and introduced a fast randomized algorithm to compute the sentinels of size $O(\frac{1}{\epsilon})$. However, Shrivastava's algorithm is limited to detecting linear cuts and fails to detect arbitrarily shaped cuts. Also, it is a centralized algorithm where information about a cut is only known to the base station.

In Ritter et al. [7], the authors select a source node and make it broadcast an *alive* message throughout the network. Border nodes detect a cut if they miss the *alive* message from the source node more than a given number of times.

The most recent cut detection algorithm is proposed by Barooah et al. [9] and overcomes several problems associated with previous solutions. Barooh's algorithm, DSSD, can not only detect an arbitrarily-shaped cut, but also