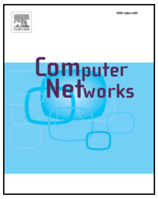
Computer Networks 126 (2017) 57–68

Contents lists available at ScienceDirect

Computer Networks

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



Reliable and energy efficient wireless sensor network design via conditional multi-copying for multiple central nodes

Merve Ekmen, Ayşegül Altın-Kayhan*

Department of Industrial Engineering, TOBB University of Economics and Technology Sögütözü 06560 Ankara, Turkey

ARTICLE INFO

Article history:
Received 29 September 2016
Revised 28 June 2017
Accepted 30 June 2017
Available online 1 July 2017

Keywords:
Wireless sensor network (WSN)
Reliability
Energy efficiency
Mixed integer programming
Multipath routing

ABSTRACT

Design of reliable wireless sensor networks considering energy efficiency is of utmost importance given their specific application domains and technical properties. As a contribution to the vast literature on resilient and fault tolerant network design, this paper offers a novel energy efficient conditional multi-copy and multi-path routing strategy. The motivation is to use limited energy of sensors as efficiently as possible and to improve network reliability and security via restricted redundant data generation. Namely, rather than all only the data passing through some *central* nodes are duplicated as a precaution against their malfunctioning. A limited number of nodes with higher data transmission allowance are determined as central at the design stage considering lifetime maximization objective. Consequently, 0–1 mixed integer programming models of two variants of the proposed strategy are presented in order to determine optimal routing. Moreover, several valid inequalities so as to improve solution times with commercial solvers and an efficient heuristic method for finding good solutions for large instances in reasonable times are proposed. Extensive test results show that simple restricted multi-copy strategies where every sensor duplicates its data are improved since the proposed strategies provide comparable levels of network reliability and yet extend network lifetime significantly.

1. Introduction

Due to their ease of implementation and ability to operate in arduous environments, wireless sensor networks (WSNs) are becoming more and more popular in numerous fields such as military, intelligent communications, health, and habitat monitoring. A WSN is composed of spatially distributed tiny electronic devices with limited energy and data processing capabilities. Each sensor collects data related to the conditions in its environment and transmits the corresponding output to a destination called the Base Station (BS) using paths determined by a routing protocol. In many applications battery replenishment is neither practical nor possible and hence it is crucial to determine transmission routes considering the efficient use of limited energy so as to prolong the network lifetime, which is mostly defined as the time until the first sensor depletes its energy or the coverage level drops under a certain threshold. In addition to energy efficient operation of a WSN, data and network integrity are two other issues of utmost importance. Given their potential deployment fields and conditions, fault tolerance and resilience of a WSN must be considered right at the design stage for improved network viability.

A WSN is fault tolerant if it continues to function when there is a disruption in some network components such as sensor malfunctions or data corruption. Efforts to design fault tolerant networks with high availability are mainly concerned with prevention, detection, or recovery dimensions. In that respect, ensuring full network coverage and connectivity during the design and deployment stages or exploiting redundancy are two main approaches for fault prevention [18]. On the other hand resilience of the network to malicious attacks such as denial of service, eavesdropping etc. is generally identified as the security of the network or intrusion tolerance. Techniques used for improving the security dimension in a WSN can be classified under five main categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection [25]. Given that sensors are mostly deployed unattended in remote places for safety critical applications, it is not surprising that there is a vast amount of work on designing available, reliable, and resilient WSNs. We cite the comprehensive surveys [1,2,18,22,25] for the interested reader.

Types of attacks to a WSN can be classified into three categories based on the respective security requirements, namely attacks on secrecy and authentication, attacks on network availability, and stealthy attacks against service integrity [25]. In this paper we will focus on secure routing, which is related with safeguarding against attacks on network integrity. Namely, we will propose

* Corresponding author.
E-mail addresses: aaltin@etu.edu.tr, aysegul6n@gmail.com (A. Altın-Kayhan).

http://dx.doi.org/10.1016/j.comnet.2017.06.028

a new energy efficient routing protocol where multi-path routing and restricted multi-copying are used for higher secrecy and availability.

In multi-path routing, each sensor can divide its data into multiple sub-packets each of which is sent to the BS on different paths [10,16,17]. Therefore, malevolent outsiders have to put more effort to capture all data pertaining to a sensor [22,23]. On the other hand, multi-copy approaches with different levels of data redundancy are available in the literature [12,15,20,21,24]. Multi-copying is beneficial for data integrity especially against injection of false packets or message corruption. Moreover, fairness of a routing in terms of balanced sensor or link utilization rates is also considered for improved network security. This is effective especially against node capture attacks since that precludes any sensor or link to be critical for data flow [18,22].

Most recently, Altın-Kayhan and Şendil [6] introduce the idea of restricted conditional multi-copying, where the balanced utilization of all sensors is provided by limiting the total amount of data each sensor would transmit for other sensors. Moreover, at most one sensor can exceed the bound only if that would be beneficial in terms of network lifetime since any data passing through that sensor must be copied at its source and sent to the BS on a node-disjoint path. The sensor with higher transmission allowance is called the central node since it is critical in communication. The main conceptual difference between the current study and [6] is the maximum number of central nodes allowed in the final design. In [6], there can be at most one central node whereas in the current work this is relaxed as not more than some integer $K > 1$. Central nodes are selected only if that would be beneficial for extending network lifetime and there is no cost incurred. Hence [6] is more restrictive in that sense. We observe in test results that more central nodes yield better lifetime values especially for larger instances. Moreover, unlike Altın-Kayhan and Şendil [6], we incorporate security for the secondary copies since we require them to be routed in balance, as well. On the other hand, technically such a relaxation in the maximum number of central nodes requires a much more complicated and elegant mathematical model, which is more challenging to solve even with commercial solvers. As a result, we offered some improvements in the way we model the problem such as tighter bounds for big M values as well as some valid inequalities. Note that the case in [6] is a special case of the strategy offered and the models in this paper can be updated accordingly to solve their problem as well. Due to the mentioned improvements, solution times as well as the linear programming bounds would be superior with the model proposed in this paper. Moreover, the heuristic proposed in Section 3 is much more generic when compared with the one in [6]. Finally, we present some test results in Section 4 so as to demonstrate the explicit improvement in lifetime due to multiple central nodes.

Central node determination is based on the intensity of data traffic through sensors, which is inspired by complex networks and their scale-free property. Complex networks are real graphs with some common important topological properties emerging because of neither random nor regular connection patterns among their components. These properties influence network availability, security, and survivability [3,4]. For instance, scale-free complex networks are the ones with a few hubs, i.e., vertices with significantly higher degrees than others. That has some implications on network integrity, namely consequences observed when a single hub fails is similar to the ones when many low-degree nodes fail. As a result, scale-free networks are prone to malicious attacks targeting hubs or functional problems due to over utilization. Based on this observation, we implement a restricted multi-copy strategy where only the data transferred over the central nodes are duplicated and routed on alternative node-disjoint paths. This idea is inspired also by the Pareto principle asserting that 80% of effects emerge due to 20% of causes. When compared with available approaches based on various levels of multi-copying, our strategy reduces data redundancy significantly while providing improved network availability since we duplicate only the data through central nodes rather than all.

In this paper we propose an energy efficient routing strategy, which ensures network integrity against attacks targeting especially some critical sensors, i.e. a fault tolerant and secure WSN. For this purpose, we require the balanced utilization of sensors in a multipath and restricted multi-copy routing scheme with conditional 2-connectivity. Basically we let a sensor use multiple paths to send its data to the BS and require only sensors utilizing any one of the multiple central nodes in transmission to produce secondary copies of just the necessary portion of their data.

The main contribution of this study to the field is a novel multipath routing strategy with conditional multi-copying and reduced data redundancy in case of multiple central nodes. In addition to the algorithmic approaches in Electrical and Electronics Engineering and Computer Science literature [8,9,11], lifetime maximization using mathematical programming is considered in the optimization literature as well [5,7,14,19]. However, to the best of our knowledge the problem of increased WSN security via optimization is not studied except [6] and [13]. We improve the strategy in [6] by allowing multiple central nodes whose number will be determined so as to maximize network lifetime. Moreover, we require balanced routing of secondary copies and present two alternative strategies varying with respect to the maximum number of central nodes that can be used for the data sensed by the same source. These differences lead not only to a more general strategy but also to more complicated mathematical models, new valid inequalities, and higher computational effort. Moreover, we briefly introduced one of the strategies mentioned in this paper in [13]. Obviously [13] is significantly extended in this paper by improving the mathematical model presented there and introducing a new alternative strategy, a new family of valid inequalities, a novel heuristic, and an extensive experimental results section covering lifetime and reliability performance comparison of the proposed strategies, impact of valid inequalities on solution times, efficacy of the heuristic as well as the sensitivity of our results to several parameters over a large sample set.

In Section 2 we define the problem and provide our mathematical models. Then we present a heuristic method in Section 3 and give an exhaustive sample of computational results in Section 4. The paper concludes with Section 5.

2. Problem definition

In this section, we will discuss our Multi-central Conditional Multi-copy Routing (CM) strategy for which we present 0–1 mixed integer programming models. The basic motivation of CM is to define a secure and energy efficient routing strategy without excessive data redundancy and to safeguard against problems which are more likely to happen and hinder network functionality significantly. For this purpose we allow multi-path routing provided that all sensors are used in balance and produce secondary copies only of data routed through the densely utilized central nodes. We show that CM provides comparable levels of network integrity with much longer network lifetime and higher amount of data sent to the BS when compared with the regular Double Copy (DC) strategy where all sensors should transmit two copies of their sensed data to the BS.

Simple example

To exemplify, we show how multi-path routing, balanced sensor utilization, and multi-copying could affect transmission routes in Fig. 1. Firstly, we have a sample network with four identical sensors and a BS denoted with a triangle in Fig. 1a. Just for simplicity