Computer Standards & Interfaces 39 (2015) 44–57

Contents lists available at ScienceDirect

Computer Standards & Interfaces

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

Evaluating energy cost of route diversity for security in wireless sensor networks

Davut Incebacak [a,*], Kemal Bicakci [b], Bulent Tavli [b]

[a] *Kocaeli University, Kocaeli, Turkey*
[b] *TOBB University of Economics and Technology, Ankara, Turkey*

ARTICLE INFO

Article history:
Received 19 February 2014
Accepted 2 December 2014
Available online 12 December 2014

Keywords:
Wireless sensor networks
Network lifetime
Network security
Eavesdropping and Node capture
Multi-path routing

ABSTRACT

Route diversity improves the security of Wireless Sensor Networks (WSNs) against adversaries attempting to obtain sensitive sensor data. By limiting the fraction of data relayed over each link and/or routed through each relay node, route diversity can be achieved, thus, extracting useful information from the network is rendered more challenging for adversaries. Sensor nodes operate with limited energy resources, therefore, energy consumption of security mechanisms is a central concern for WSNs. In this paper we evaluate the energy cost of route diversity for security in WSNs through a novel Linear Programming framework. We characterize energy dissipation and data relaying behaviors of three route diversity techniques to mitigate node capture only, eavesdropping only, and node capture and eavesdropping attacks. Effects of node density, network area, level of resilience, and network topology on energy cost are investigated.

1. Introduction

Wireless Sensor Networks (WSNs) are composed of small form factor devices (nodes) that are instrumented with different types of sensors to carry out certain sensing tasks within a designated operation area. With limited computation and energy resources, nodes are capable of sensing physical phenomena, processing the sensed data, and transmitting the information. Being densely deployed, nodes cooperate with each other to achieve the assigned tasks. For example, cooperation in conveying sensed data towards the base station is achieved using other nodes as relays. Self organization and infrastructureless characteristics of WSNs make them promising solutions for surveillance and control tasks [1,2]. Since WSN characteristics are suitable for utilization in hostile environments, they are invaluable assets for tactical communication and networking in military applications.

Security is a critical issue for WSNs because nodes usually operate unattended and communication takes place in a broadcast medium. A common and successful technique used against eavesdropping is cryptographic encryption. With encryption, sensor data is scrambled using a key to make eavesdropped data unintelligible to anyone who does not possess the key. However there is always a possibility that a single technique may be flawed or cracked (e.g., IEEE 802.11 WEP protocol). Moreover, in WSN sensor nodes can be captured (i.e., node capture attacks) and vital cryptography information such as keys can be extracted from them. If keys are captured, this would render the encryption useless. Eavesdropping attacks are usually unnoticed (i.e., it is challenging to detect a passive attack), thus, these attacks can succeed without encountering any active defense [3]. Layered approach to security and “defense-in-depth” strategy mandate that alternative or complementary techniques be used.

Security can be enhanced by using route diversity (i.e., multi-path routing) which exploits multi-hop characteristics of WSNs by providing multiple paths between the source node and the base station to split data on these paths. Route diversity can be used as a standalone security countermeasure or in conjunction with encryption. While encryption is a good defense against attackers who are already eavesdropping wireless transmission, route diversity makes eavesdropping more difficult in the first place[1] [3]. By splitting data along different paths, an adversary has to capture portions routed through different paths to construct one node's data which requires more effort than extracting information in a single path case. In other words, an adversary needs to spend more resources to collect data from the network if route diversity is implemented.

Lifetime optimization of WSNs is one of the most important functional design objectives because WSNs are envisioned to be operating in hostile and harsh environments where human intervention is risky or costly. In such environments, battery replenishment is not possible or highly challenging. Adding security capabilities to a WSN without considering energy efficiency can lead to inefficient energy dissipation

* Corresponding author.
E-mail addresses: davut.incebacak@kocaeli.edu.tr (D. Incebacak), bicakci@etu.edu.tr (K. Bicakci), btavli@etu.edu.tr (B. Tavli).

[1] While route diversity can also be useful against denial of service attacks [4], our main motivation in this paper is to study it in the context of data confidentiality.

http://dx.doi.org/10.1016/j.csi.2014.12.003
0920-5489/© 2014 Elsevier B.V. All rights reserved.

characteristics in the whole network and network lifetime can decrease dramatically. Thus, while enhancing WSN security, energy requirements should not be overlooked.

Our goal in this paper is to investigate the energy impact of route diversity countermeasures in WSNs. There are at least two types of energy overhead route diversity brings. First of these is due to the need to discover, establish, and maintain multiple routes instead of a single route between sensor nodes and the base station. In WSNs consisting of stationary nodes, this is a one-time operation for a substantial amount of time [5], hence, can be ignored. There is a second factor which makes the energy cost of route diversity more than the energy cost of single route paradigm. When data is split into multiple parts and forwarded via multiple routes, it is no longer possible to carry all data in energy-optimal paths. Some portion of the data should be transmitted towards the base station via less efficient paths. In fact, all routes can be sub-optimal from an energy efficiency perspective when compared to a single energy-efficient route. Broadly speaking, we can say that the second factor is more significant than the first one because it is applicable not only for a limited period of network operation but during the entire network lifetime. In other words, since WSNs generally exhibit stationary topology and connectivity behavior, route updates are infrequent. On the other hand, data transport by using multiple paths is a continuous operation spanning the entire network lifetime.

While it is tempting to state that the energy cost of route diversity is high, we are not aware of any clear scientific evidence or convincing analysis to support such a claim. It can also be argued that (with equal lack of convincing scientific evidence) the energy cost associated with route diversity is small and can easily be neglected. Given the fact that without a proper analysis it is not possible to quantify or even give a rough estimate on the energy cost of route diversity, in this paper we make the first attempt to carry out an analysis on this subject by building a framework using Linear Programming (LP). LP is a technique to solve the problem of maximizing or minimizing a linear function whose variables are required to satisfy a finite set of constraints that are expressed either as linear equalities or linear inequalities. In the context of WSNs, LP approach has previously been applied in many studies to model the unique characteristics of WSNs and to determine the optimal solutions to problems that are specific to WSNs (e.g., [6–15]).

Choosing an LP based analysis method has a number of advantages. One of them is the abstraction from a specific protocol which enables us to investigate energy cost in ideal conditions with optimal routing decisions. Secondly, due to global knowledge in the optimization problem solver, the results can be obtained in an efficient and consistent manner.

In this study, we consider a WSN where nodes have sensitive data to be conveyed to the base station. Data is spread out on multiple paths to mitigate both active and passive attacks. Data flows on these paths are optimized to minimize the overall energy consumption throughout the network. Furthermore, to avoid premature death of any node within the network energy dissipation is evenly balanced throughout the network, hence, the network lifetime is optimized. Within an LP framework, we model the energy dissipation characteristics of route diversity countermeasures against node capture (NCO), eavesdropping (EAO), and both node capture and eavesdropping (NCE) attacks. Using the developed LP models, we evaluate the energy cost of these countermeasures by benchmarking against the energy requirements of unconstrained optimal case.

The remainder of this paper is organized as follows. Related work is presented in Section 2. Security assumptions, threat model, system model, and LP formulations are presented in Section 3. Results of analysis based on LP models are presented in Section 4. The discussion of models, assumptions, analysis and implications of the results, and promising future directions are presented in Section 5. Concluding remarks are made in Section 6.

2. Related work

The literature on multi-path routing is extensive and has grown rapidly in recent years. Providing a comprehensive overview of the published research on multi-path routing is beyond the scope of our work. We refer interested readers to the recent surveys on this topic [16,17]. Nevertheless, we present a brief overview of the literature on multi-path routing by summarizing the studies most related to our work.

We first note that multi-path routing provides several attractive properties other than security such as load balancing, reliability, and quality of service support [16]. Multi-path routing can be used to improve the lifetime of WSNs by enabling balanced energy dissipation throughout the network. Consider the case where each node has a single path to the base station, which leads to energy imbalances throughout the networks (i.e., relay nodes on heavily utilized paths dissipate more energy than the other nodes). Sending data in multiple paths can be used to balance energy dissipation and prevents premature deaths of nodes on certain paths (e.g., minimum-energy path, minimum-hop path). There are several studies which address the problem of imbalanced energy dissipation by designing protocols that use multiple paths (e.g., [18–20]).

As a second note, we state that there are several related concepts in this area which can also be named as multi-path routing and may be confused with the meaning of multi-path routing as it is used in this paper. In this paper, we use the terms multi-path routing and route diversity interchangeably[2] and refer to splitting the data into parts without employing data redundancy and sending each part via a different path towards the base station. Alternate path routing is different than multi-path routing in the sense that a single path is used in normal operation but alternative paths are kept ready to be used in case the primary path becomes unavailable [22]. Redundant multi-path routing is another related term that means the data to be conveyed to the base station is transported via multiple paths with added redundancy (e.g., multiple replicas of the data is sent on different paths). From security point of view, adding redundancy is useful for enhancing resilience against denial of service attacks [4].

Important problems in multi-path routing research include discovering multiple paths, selecting a number of paths among them, and distributing load across these selected paths [17]. In the following paragraphs, we provide brief summaries of some exemplary protocols which focus on one or more of these problems in the context of security and by considering attack resistance property.

In [23], the problem of data distribution across multiple paths is studied with the aim of minimizing the maximum damage when a single link attack occurs in the network. The solution is formulated as a maximum-flow problem that can be solved in a distributed fashion.

In [24], a secure method for choosing multiple paths and distributing data among these paths is presented. The design objective is to minimize the percentage of captured data by an adversary. Each path is assigned with a security parameter that identifies the past performance on reliable data delivery. According to these parameters, multiple paths are constructed and data is distributed among these paths using min–max optimization and game theory.

In [25], an on-demand secure multi-path routing protocol is proposed to protect communication against collaborating malicious nodes. The protocol includes two phases. The first phase achieves neighbor node authentication by Elliptic Curve Cryptography. In the second phase, node-disjoint paths are found between source and destination nodes.

In [26], data is divided into parts and encrypted combinations of these are sent on different paths. Two of the paths are used for signaling and key sharing, thus, at least three paths between source and

[2] We prefer to use the term "route diversity" in the title because we think it better reflects our focus on security in this paper. For a general discussion on the role of diversity in security, see [21].