Ad Hoc Networks 37 (2016) 301–323

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Maximizing Wireless Sensor Network lifetime by communication/computation energy optimization of non-repudiation security service: Node level versus network level strategies

Huseyin Ugur Yildiz [a,*], Kemal Bicakci [b], Bulent Tavli [a], Hakan Gultekin [c], Davut Incebacak [d]

[a] Electrical and Electronics Engineering, TOBB University of Economics and Technology, 06520, Ankara, Turkey
[b] Computer Engineering, TOBB University of Economics and Technology, 06520, Ankara, Turkey
[c] Industrial Engineering, TOBB University of Economics and Technology, 06520, Ankara, Turkey
[d] Computer Engineering, Kocaeli University, 41380, Kocaeli, Turkey

ARTICLE INFO

Article history:
Received 16 February 2015
Revised 31 July 2015
Accepted 27 August 2015
Available online 11 September 2015

Keywords:
Wireless Sensor Networks
Digital signature
Network lifetime
Energy efficiency
Mixed Integer Programming
Heuristic

ABSTRACT

In a typical Wireless Sensor Network (WSN) application, the basic communication service is the transportation of the data collected from sensors to the base station. For prolonging the network lifetime, energy efficiency should be one of the primary attributes of such a service. The amount of data transmitted by a node usually depends on how much local processing is performed. As an example, in visual sensor networks the amount of image processing on the nodes affects the amount of data transmitted to the base station (*i.e.*, the higher the computation, the lower the communication and vice versa). Hence in order to improve energy efficiency and prolong the network lifetime this communication/computation energy trade-off must be analyzed. This analysis may be performed at the network-level (*i.e.*, all nodes in the network use the same strategy) or at a node level (*i.e.*, sensor nodes do not necessarily have identical strategies). The latter is more fine-grained allowing different nodes to implement different solutions. To guide designers in effectively using these trade-offs to prolong network lifetime, we develop a novel Mixed Integer Programming (MIP) framework. We show that the optimal node level strategy can extend network lifetime more than 20% as compared to a network-level optimal strategy. We also develop a computationally efficient heuristic to overcome the very high computational requirements of the proposed MIP model.

1. Introduction

Wireless Sensor Networks (WSNs) consist of a plurality of sensor nodes deployed over a geographical area which are, typically, equipped with low computational capacity processors, short range wireless transceivers, and limited energy resources (*i.e.*, batteries) for monitoring physical phenomena like temperature, humidity, acoustic vibrations, and light intensity [1]. Note that there are also WSNs consisting of mobile nodes [2], however, in this study we only consider WSNs with stationary nodes. Communication and computation are the two main energy consumption categories for a typical WSN, communication energy is, usually, assumed to dominate the energy expenditure of the sensor nodes [3]. The se-

* Corresponding author. Tel.: +90 312 555 63 04.
E-mail addresses: huyildiz@etu.edu.tr, huguryildiz@ieee.org (H.U. Yildiz), bicakci@etu.edu.tr (K. Bicakci), btavli@etu.edu.tr (B. Tavli), hgultekin@etu.edu.tr (H. Gultekin), davut.incebacak@kocaeli.edu.tr (D. Incebacak).

http://dx.doi.org/10.1016/j.adhoc.2015.08.026
1570-8705/

Table 1
Acronyms used in this paper.

Acronym	Description
DS	Digital Signature
WSN	Wireless Sensor Network
OTS	One Time Signature
RSA	Rivest–Shamir–Adleman
ECDSA	Elliptic Curve Digital Signature Algorithm
LP	Linear Programming
MIP	Mixed Integer Programming
GSS	Golden Section Search
SA	Simulated Annealing

vere energy constraints imposed on WSNs lead designers to endeavor for energy efficient operation strategies and algorithms. Therefore, maximizing network lifetime by optimizing the energy dissipation of sensor nodes is considered to be the most important design goal for WSNs [4]. In this study, similar to [3,5], and [6], the network lifetime is defined as the duration between the time network starts operating and the time when the first sensor node in the network exhausts all its energy and dies. The acronyms used throughout the text are explained in Table 1.

We consider the following scenario to motivate our work. A WSN is deployed for surveillance purposes. Each node has a built-in camera periodically capturing still images. Transportation of data from the sensor nodes to the base station may involve the other nodes acting as relays (multi-hop communication). The base station processes the collected data and interacts with a user. We note that since image processing requires the use of complex algorithms, visual sensor nodes dissipate significantly higher power than scalar nodes. Besides, bandwidth requirements for carrying visual data are also much higher [7]. As a result, exploiting the communication/computation energy optimization tradeoff is more prominent in visual sensor networks.

In such an application, if the design goal is to prolong the network lifetime, then the following question becomes highly relevant. How much processing should be performed locally on the nodes? On one extreme, there may be no local processing at all and nodes simply transmit raw images. On the other extreme, nodes may run the most sophisticated image processing and machine vision algorithms so that only minimal amount of data is transmitted to the base station (*e.g.*, only semantic data pertaining to a suspicious situation). Other options may lie in the middle with a moderate amount of local processing (*e.g.*, images may be compressed before transmission).

Unlike computational costs, energy consumption of communication cannot be expressed with a simple formula because it depends not only on the distance between the node and the base station but also on the exact route taken which is not necessarily the shortest hop route or the minimum energy path. A Linear Programming (LP) model with the objective of maximizing the lifetime has been proposed in an earlier work [4] which can be used to analyze the trade-off exemplified above. However, there is one issue which has not been investigated yet. Instead of adopting a single processing option applied to all nodes in the network, we may implement a hybrid solution, in which different nodes may use different processing options.

To explain this problem in more concrete terms, in our work we analyze non-repudiation security service[1] which has the highest energy overhead [8,9] among all security-related techniques in WSNs [4]. Digital signature *(DS)* algorithms that could be used to implement a non-repudiation service include widely adopted Rivest–Shamir–Adleman *(RSA)* algorithm [10], Elliptic-Curve Digital Signature Algorithm *(ECDSA)* [11]—a robust and efficient alternative to RSA, and One-Time Signature *(OTS)* algorithm [4,12] having a unique trade-off between computation and communication with its long signature sizes and practically zero computational cost.

Since ECDSA has better performance figures than RSA algorithm in terms of both computation and communication (see Table 3), we can easily say which one is more energy-efficient. On the other hand, as mentioned, it is not straightforward to tell whether ECDSA or OTS algorithm should be preferred in a given application. The problem becomes even more complicated if we may have the option to perform the processing (for generating ECDSA signatures) only in a subset of nodes in the network but not in the remaining ones (where OTS is used).[2]

In this paper our objective is to seek answers to the following research problems:

1. How much improvement in terms of network lifetime can we attain with a strategy in which different nodes may implement different options instead of all nodes use the same option? In more concrete terms, what is the impact of assigning a single digital signature algorithm to all nodes in the network globally instead of choosing the optimal algorithm for each node, separately?
2. Can we build a mathematical programming framework to uncover the research challenge posed in Question (1) without any optimality gap?
3. Is it possible to develop a computationally efficient heuristic algorithm which closely approximate the exact solution for the research problem in Question (2)?

To answer Questions (1) and (2), we build a novel Mixed Integer Programming *(MIP)* framework. The computational complexity of the MIP model [13,14] lead us to develop heuristic methods for finding an answer to Question (3). Heuristic methods are commonly used in applied optimization [15,16]. Their main purpose is to ensure that optimization problems are solved in reasonable time (*i.e.*, reduce computational complexity) by providing feasible solutions close to the optimal solution, but without any guarantee of finding the exact optimal.

The rest of this paper is organized as follows: Section 2 summarizes the related work and our original contributions. Section 3 presents the MIP framework. Section 4 presents the results of numerical analysis of the MIP model. In Section 5, two heuristic algorithms are presented and their

[1] An example regarding security is chosen due to availability of energy overhead information from previous work [4] but our framework could be easily tailored to analyze other computation/communication trade-offs once the required numerical data are available.

[2] We acknowledge that this node level strategy brings additional complexity and may not always be applicable.