Journal of Information Security and Applications 52 (2020) 102467

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Trust-aware and cooperative routing protocol for IoT security

Nabil Djedjig[a,b,*], Djamel Tandjaoui[a], Faiza Medjek[a,b], Imed Romdhani[c]

[a] Research Centre on Scientific and Technical Information, 03, Rue des Freres Aissou, Ben Aknoun, Algiers, Algeria
[b] Departement Informatique, Faculte des Sciences Exactes, Universite de Bejaia, Bejaia 06000, Algeria
[c] Edinburgh Napier University, School of Computing, 10 Colinton Road, Edinburgh, EH10 5DT, UK

ARTICLE INFO

Article history:
Available online 28 February 2020

Keywords:
RPL
Secure routing
Internet of things
Trust management
Game theory
Cooperation enforcement

ABSTRACT

The resource-constrained nature of IoT objects makes the Routing Protocol for Low-power and Lossy Networks (RPL) vulnerable to several attacks. Although RPL specification provides encryption protection to control messages, RPL is still vulnerable to internal attackers and selfish behaviours. To address the lack of robust security mechanisms in RPL, we design a new Metric-based RPL Trustworthiness Scheme (MRTS) that introduces trust evaluation for secure routing topology construction. Extensive simulations show that MRTS is efficient in terms of packet delivery ratio, energy consumption, nodes' rank changes, and throughput. In addition, a mathematical modelling analysis shows that MRTS meets the requirements of consistency, optimality, and loop-freeness and that the proposed trust-based routing metric has the isotonicity and monotonicity properties required for a routing protocol. By using game theory concepts, we formally describe MRTS as a strategy for the iterated Prisoner's Dilemma and demonstrate its cooperation enforcement characteristic. Both mathematical analysis and evolutionary simulation results show clearly that MRTS, as a strategy, is an efficient approach in promoting the stability and the evolution of the Internet of Things network.

1. Introduction

The Internet of Things (IoT) is a new communication paradigm that affects our daily lives in many domains, such as healthcare, home and building automation, automobiles, urban, and industrial appliances. IoT-based networks are more likely formed of Low-power and Lossy Networks (LLNs), which are composed of various heterogeneous wireless technologies (objects), such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, etc. In these technologies, computing and communication systems are seamlessly embedded [1]. IoT's objects are characterised both by their strong resource constraints and by their lossy communication links. Indeed, these objects have limited processing power, memory, and energy supply, in addition to a high loss rate, a low throughput, a limited frame size, and short communication ranges [2,3]. Such limitations raised several challenges for industry and academic research community, for example, scalability, routing, and security.

This last decade, several routing solutions for LLNs were suggested. Finally, the Internet Engineering Task Force (IETF) ROLL (Routing Over Low power and Lossy networks) [4] working group has developed and standardised the Routing Protocol for Low-power and Lossy Networks (RPL) [5]. One major issue for the IoT is the routing's security that researchers consider as a critical requirement [3,6]. Even though the RPL specification defines cryptography-based mechanisms to ensure control messages integrity and confidentiality against outsider attackers [5], RPL is still vulnerable to various known and new internal threats, that have been extensively studied in the literature [7,8].

Trusting the objects participating in the routing process is crucial for the proper functioning of the network. For this reason, we focus our research study on addressing RPL weaknesses in terms of routing security by proposing a security scheme for RPL based on trustworthiness between nodes. In this paper, we introduce a Metric-based RPL Trustworthiness Scheme (MRTS) that enables secure routing by avoiding malicious nodes, and calculating and choosing the most trusted path from the source node to the root. We introduced MRTS initially in [9]. Firstly, this paper is a revision of our previous work [9] where new elements and components are added to enhance MRTS performance in terms of security, lifetime and routing Quality of Service (QoS). Secondly, this paper extends the work in [9] with a simulation validation and a mathematical analysis.

Cooperation and collaboration are considered critical in the development of trust relationships among participating nodes for secure operations of the network [10]. According to

* Corresponding author.
E-mail address: djedjig_nabil@cerist.dz (N. Djedjig).

https://doi.org/10.1016/j.jisa.2020.102467
2214-2126/