Journal of Network and Computer Applications 66 (2016) 198–213

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Secure routing for internet of things: A survey

David Airehrour [a,*], Jairo Gutierrez [a], Sayan Kumar Ray [b]

[a] School of Engineering, Computer and Mathematical Sciences, Auckland University of Technology, Auckland, New Zealand
[b] Faculty of Business and Information Technology, Manukau Institute of Technology, Auckland, New Zealand

ARTICLE INFO

Article history:
Received 16 December 2015
Received in revised form
17 February 2016
Accepted 8 March 2016
Available online 10 March 2016

Keywords:
IETF
6LoWPAN
RPL
IEEE 802.15.4
IoT
Routing
Security
Sensors

ABSTRACT

The Internet of Things (IoT) could be described as the pervasive and global network which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. It is projected that by 2020 the number of connected devices is estimated to grow exponentially to 50 billion. The main drivers for this growth are our everyday devices such as cars, refrigerators, fans, lights, mobile phones and other operational technologies including the manufacturing infrastructures which are now becoming connected systems across the world. It is apparent that security will pose a fundamental enabling factor for the successful deployment and use of most IoT applications and in particular secure routing among IoT sensor nodes thus, mechanisms need to be designed to provide secure routing communications for devices enabled by the IoT technology. This survey analyzes existing routing protocols and mechanisms to secure routing communications in IoT, as well as the open research issues. We further analyze how existing approaches ensure secure routing in IoT, their weaknesses, threats to secure routing in IoT and the open challenges and strategies for future research work for a better secure IoT routing.

1. Introduction

With the advancement in mobile computing and wireless communications, a new paradigm known as the *Internet of Things* (IoT) is swiftly generating a lot of research interest and industrial revolution. The *Internet of Things* (IoT) could be described as the pervasive and global network, which aids and provides a system for the monitoring and control of the physical world through the collection, processing and analysis of generated data by IoT sensor devices. These devices have built-in sensing and communication interfaces such as sensors, radio frequency identification devices (RFID), Global Positioning devices (GPS), infrared sensors, laser scanners, actuators, wireless LANs and even Local Area Networks (LANs) interfaces (Zhao and Ge, 2013). These "*things*" can be connected to the internet and hence could be controlled and managed remotely. These devices could interact among themselves (Machine-to-Machine (M2M)) by way of sending and receiving information, sensing the environmental temperature, pressure etc. while transmitting same to other devices for further processing or other actions (Xu et al., 2013; Wei and Qi, 2011). According to International Telecommunications Union (ITU) and the *IoT European Research Cluster* (IERC) the Internet of Things (IoT) is defined as a vivacious worldwide network infrastructure with self-configuring capabilities centered on standard and interoperable communication protocols in which physical and virtual "things" have identities, physical features and virtual characteristics, communicate via intelligent interfaces and integrate into the information network in a seamless fashion (Fig. 1).

IoT can be viewed as a fusion of heterogeneous networks that brings not only the same security challenges present in sensor networks, mobile telecommunications and the internet but also some peculiar and accentuated issues, like, network privacy problems, authentication on a heterogeneous network, access control challenges and secure routing among these heterogeneous devices (Zhao and Ge, 2013).

The IoT has, in the last few years, become a topical issue in academia and industry. While becoming increasingly ubiquitous, IoT supports a comprehensive representation of the physical environment and a good level of interaction with the physical world (Atzori et al., 2010; Gubbi et al., 2013). Areas such as logistics, intelligent transportation systems (ITS), business/process management and e-health are just few instances of conceivable application fields where this novel paradigm will be highly useful. The realization of IoT will greatly hinge on various criteria such as the system's architecture, networks and communications, data processing, and ubiquitous computing technologies which support efficient, reliable, physical and cyber interconnectivity. A fundamental driving force of IoT that facilitates the interconnection of devices is networking, and specifically, routing in the network. It involves the creation of traffic routes, and transmitting the routed packets from source to final destination in a network. With billions

* Corresponding author.

http://dx.doi.org/10.1016/j.jnca.2016.03.006
1084-8045/

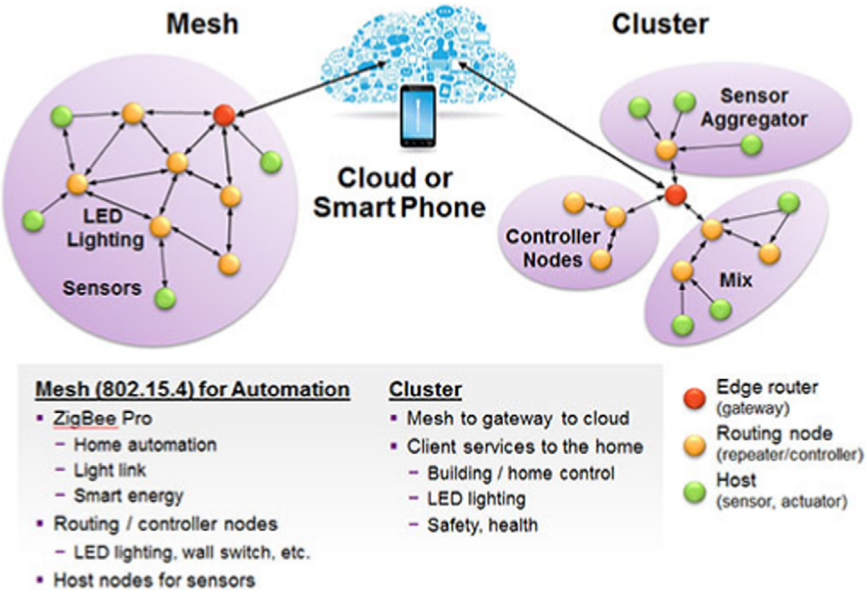

Fig. 1. An interconnectivity of IoT nodes comprising of edge routers (gateway to the cloud), routing nodes (that also serve as control nodes) and mobile sensory or actuator nodes (Spansion, 2014).

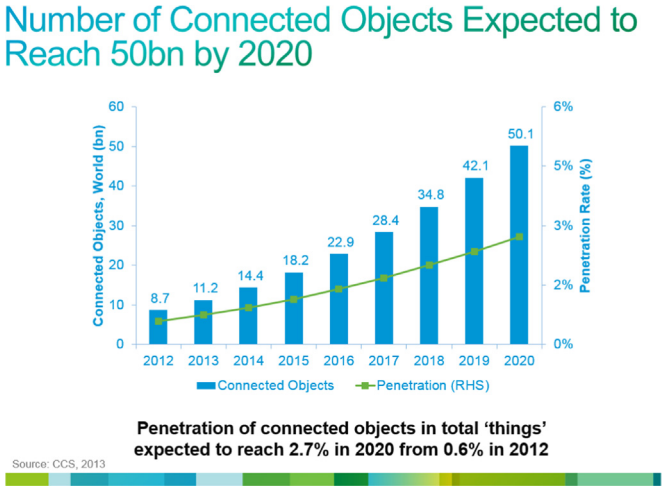

Fig. 2. A forecast of more than 50 billion interconnected devices by 2020: Source (CISCO, 2013).

of devices interconnected in the network, an uphill challenge is securing the network from various forms of threats and attacks. Users will feel insecure about their private data if they are vulnerable to attacks from unauthorized individuals or machines over the network. With 50 billion interconnected IoT nodes, as shown in Fig. 2, security is by far one of the biggest challenges in IoT networks (Evans, 2011; Ericsson, 2011; CTIA-The Wireless Association, 2014).

Sequel to our discussions above, routing and addressing are critical issues in IoT owing to the requirement of maintaining a uniformity in the way packets are routed between source and destination between IoT devices traveling across varying network topologies. Making the process of routing secure enough in IoT is even more challenging (Gubbi et al., 2013). This imperative need for securing the routing process between numerous IoT devices across multiple heterogeneous networks needs significant research contributions. Current research findings show that IT security threats for 2013–2015 are threats that subsist only with the presence of a network and they include: botnets, malware, Denial-of-Service (DoS) attacks on financial services and Distributed Denial of Service (DDoS) attacks, web-based malware, android malware and Spam (Mc Afee Labs, 2014; Sophos Limited, 2013, 2014).

In this survey, we explore the IoT routing protocols in general and discuss few of the key secure IoT routing protocols and their vulnerabilities to attacks during routing. The contribution of this paper is threefold. First, we introduce the Internet of Things and its relevance as well as growing trends in today's global IT scenario. Second, the paper gives an overview of the threats associated with IoT routing and identifies few of the research challenges as discussed by the research fraternity. Lastly, the paper briefly highlights some of the potential research directions in achieving secure and sustainable routing among IoT devices. To the best of our knowledge, this survey paper is the first of its kind intending to provide researchers and readers a broad overview on the different research findings and proposed solutions on the issue of secure routing among IoT devices. The rest of the paper is organized as follows. Section 2 briefly talks about the security and energy consumption in IoT networks. The routing protocols are discussed in Section 3. This is followed by Sections 4 and 5 that, respectively, discuss the vulnerabilities to IoT routing and trust in IoT secure routing. An overview of the issues and challenges of secure routing in IoT is provided in Section 6 and finally, in Section 7 we conclude the survey.

2. Security and energy consumption: where the need lies in IoT?

IoT has many promising areas of application including commercial (oil well sensing, intelligent vehicular transportation system, gaming, and agriculture), smart homes, wearables, healthcare, automotive industries and the power smart grid system. To maintain the seamless functioning of the IoT networks, the areas of primary focus in IoT research are the (a) security (including the communication between sensor nodes) and (b) energy consumption of the different IoT nodes. In the following sub-sections, we explore these two aspects that will play key roles in the IoT revolution.