International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 7, No.2 (Mar-2018)
http://dx.doi.org/10.12785/ijcds/070206

Internet of Things Security Issues, Threats, Attacks and Counter Measures

Adil Bashir[1] and Ajaz Hussain Mir[1]

[1]*Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, Jammu & Kashmir, India*

Received 11 Oct. 2017, Revised 30 Nov. 2017, Accepted 26 Jan. 2018, Published 1 Mar. 2018

Abstract: Internet of things (IoT) is gaining popularity now-a-days as it is revolutionizing the world of internet and physical systems in a more advanced and technical way. IoT consists of physical things in which sensing, processing and communication capabilities are added. These devices have restricted resources and processing competences. The networks formed from these miniature devices have a lot of scope and applications that include healthcare, industrial automation, military surveillance, forest fire detection, flood alarming system, smart homes, smart cities etc. Most of these applications demand secure transmission of sensed information from source IoT node to gateway node or broker. Thus, it is imperative to pay attention to the security of these networks as they are highly susceptible to risks because of wireless medium used for communication and the constrained nature of these devices. In this paper, we have presented a variety of attacks that can harm the fidelity of transmitted information in IoT, thereby generating unauthorized effects. Furthermore, various counter measures against these possible attacks that have been proposed in the literature with their merits and demerits are presented, together with possible research opportunities for future work.

Keywords: Internet of Things Security, MQTT, CoAP, RPL, Wireless Sensor Networks.

1. INTRODUCTION

T Internet of Things (IoT) encompasses a large set of devices compromising of sensing, computation and communication components having resource restrictions [1]. These devices are capable of sensing, monitoring, self-organizing and find their usage to sense the ambient condition of its environment, assemble data, and process it to extract some significant information that can be used to identify the event in the region of its surroundings. A node is the prime component of IoT network which is built of sensing, computation and wireless communication components with an on-board battery. Internet of Things lets devices to act automatically to events and changes in their surroundings without any human interaction [2]. Due to small size, quick and easy deployment and low cost of IoT nodes, it becomes possible to deploy them in a hefty area to be examined [3]. IoT nodes are typically spread over the area to be observed to collect data, process it, and forward it to the gateway directly or through multi-hop communication for further processing. Cisco estimates that the Internet of Things will grow to almost 50 billion installed units by 2020 [4]. Advances in communication technology and Micro-Electro-Mechanical Systems (MEMS) result in lowering deployment and maintenance costs of IoT and reduces susceptibility rate of node to failures with an improved battery power. Therefore, these networks find their applications in monitoring smart homes [5] or healthcare [6], assisted living, enhanced learning [7], supply chain management etc. For example, a smart door lock installed at home/apartment communicates its status to the user's smart-phone. The user can access the status of smart door lock sensor from anywhere in the world which enables him to verify, for example, if he forgot to lock the door of house before leaving, or if a robbery was attempted.

Internet of Things has a three layered architecture [8]. The three layers include Physical/ perception layer, network layer and application layer.A typical IoT architecture looks as illustrated in Figure 1.

The Physical layer or perception layer has sensors for accumulating data from environment. It senses physical parameters and shares this collected data to other smart objects. Low energy communication protocols and technologies such as IEEE 802.15.4 [9] [10], ZigBee [11], ISA 100.1a [12], WirelessHART [13] are utilized to transmit sensed data to other IoT objects.

Network layer consists of low-power routing protocols such as RPL (Routing Protocol for Low power and Lossy Networks) [14] for communication with other IoT nodes. Usually gateways are used between local

E-mail:adilbashir.445@gmail.com, ahmir@nitsri.net