Chapter 3
Security in Network Layer of IoT: Possible Measures to Preclude

B. Balamurugan
VIT University, India

Dyutimoy Biswas
VIT University, India

ABSTRACT

The internet of things (IoT) is an imminent model in the field of wireless telecommunications. It is also considered as a third wave of information technology after the Internet and mobile communication. Basically, IoT is a wireless interconnected network of variety of objects such as radio frequency identification (RFID) tags, sensors, actuators, mobile phones and other types of wireless devices. It has extensible application in the areas such as public security, infrastructure development, modern agriculture, environment protection, urban management, healthcare, enhanced learning, and business service, among others. IoT is a self-configuring wireless network of sensors where the primary goal of establishing connection is to offer interconnectivity of various objects. The concept of IoT was coined by the Auto-Id center of the Massachusetts Institute of Technology (MIT) in 1999.

DOI: 10.4018/978-1-5225-2296-6.ch003
INTRODUCTION

Internet of things (IoT) is an amazing, if not the most powerful technological invention of the last couple of decades, providing superior power to the hands of human race. The most promising aspect of IoT is that this technology is still budding and has immense potential to kick-start a new, fully coordinated technological era. In IoT, ‘things’ or devices communicate between each other over wireless networks. Therefore, while developing algorithms and techniques for IoT, the standards and rules set for wireless networks, which are essentially different from that of wired networks, are taken into consideration. Since IoT is still in its inception stage, its usage is still limited within the scope of the enterprises and not very common in consumer market. Therefore, unlike the high speed network where computers communicate with other computers where aspects of ‘security breaches’ is dealt by the programmers and developers for ages, and many robust techniques for this purpose have been built and used, in IoT, with fewer, if not zero, number of cases of security breaches have occurred, apart from standard techniques, it’s a challenge for the engineers to develop techniques, both on hardware and software levels, to secure the future of IoT (Kelly et al., 2013; Babar et al., 2010; Alam, Sarfraz, Chowdhury, & Noll, 2011; Barnaghi et al., 2012).

In IoT, the new objects that enter the network are configured automatically. This characteristic makes IoT highly susceptible to security threats. Among several kinds of threats in an IoT network, Disruption and Denial of Service (DoS), eavesdropping, problems in authentication and physical attacks on devices in different forms, are most common.

Therefore, it is essential to devise security measures without interfering with the operation of the IoT network. Also, robust and bug-free analytical tools and algorithms should be employed that will detect malicious and unethical activity, whilst improving service offered to the customers. Generally, the intrusion detection and prevention systems and enhancement of packet security by incorporating suitable fields in packet header are the security measures associated with the Layer 3 of wireless networks (Babar et al., 2010; Zargar et al., 2013; Savola, Reijo, Abie, & Sihvonen, 2012).

SECURITY ISSUES

Ensuring security for the IoT devices has been the most challenging task. Combining a strong cryptography with a highly constrained environment, under the condition of limited energy consumption, since most of the devices are battery operated, and little or no maintenance time makes it extremely difficult. That IoT can achieve
Optimal Strategy in Queueing Systems in Emergency Department
www.igi-global.com/article/optimal-strategy-in-queueing-systems-in-emergency-department/193010?camid=4v1a

Web 3.0 in Web Development
www.igi-global.com/chapter/web-30-in-web-development/127291?camid=4v1a