Chapter 51
Efficient Routing Protocol for Location Privacy Preserving in Internet of Things

Rajwinder Kaur
Central University of Rajasthan, Ajmer, India

Karan Verma
Central University of Rajasthan, Ajmer, India

Shelendra Kumar Jain
https://orcid.org/0000-0002-9692-9505
Central University of Rajasthan, Ajmer, India

Nishtha Kesswani
Central University of Rajasthan, Ajmer, India

ABSTRACT

Internet of Things is a norm which has expanded very swiftly with high magnitude of heterogeneity and functionalities. Security and privacy became the prime factors of Internet of Things due to unsecured character of wireless communication. Thus, because of unsecured network, it is easy for invaders to trace and find the position of nodes during communication and leak the information. Issues related to location information may include sharing of information, storage, sensing, and processing which can be used by external entities in different contexts, i.e. contexts can be: technical, legal, and social. These issues make privacy a major concern. Here, the research this article presents notions of existing privacy models and the amplified techniques using a random path. The article then describes possible solutions to preserve the location of nodes with less transmission time. Results of proposed scheme depict effectual behavior of the approach.

DOI: 10.4018/978-1-7998-8954-0.ch051

INTRODUCTION

Internet of Things is a norm of connecting the whole world through network with the help of sensors, different telecommunication interfaces which are entirely dependent upon wireless technologies. RFID (Radio Frequency Identification), WSN (Wireless Sensor Networks) (Sicari et al., 2015) and NFC (Near Field Communication) technologies are playing a pivotal role in Internet of Things (IoT) infrastructures. The concerns of the Internet of Things are to allow things to be connected ubiquitous (anytime, anyplace, with anything and anyone) or preferably using any path/network and any service. Thus, the main objective of the IoT is to provide better quality of services to users and to mark down the cost of resources can act as an important step close to "Smart World" (Vasilomanolakis et al., 2015). Smart City is the bigger part of IoT and it includes smart communication, emergency management, health monitoring, smart vehicle parking, smart roads, context-based vehicle maintenance, smart waste management, smart grid, smart retails and many more applications. In the scenario of IoT, all the objects connect probably with the internet which creates the interconnection between the two things which may be of type: M to M, M to H or H to H communication where M is machine and H is Human. For the connectivity and sensibility, sensors used in these technologies which also observe different surroundings like humidity, motion, and climate in the communication. These sensors nodes in Internet of Things, are connected to a central system which stores the plethora of data and then just provide various data access to all devices. This stored data can leak the private data which can create privacy issues for a user. If we talk about privacy in health-care system using IoT, patient transfer information like address, name, health statistics which is a most sensitive data, can be accessed by unauthorized third party and can be leaked (Airehrour et al., 2016).

According to IoT theory, everything turns into virtual world that means every single person and thing are addressable, locatable and readable on the internet. Thus, IoT things may have some characteristics e.g. connectivity, dynamicity, existence, privacy, interactivity and sensibility. As a consequence, it became mandatory to preserve the location privacy of node in Internet of Things because if location gets drained, invader can smoothly destroy the source node and sink node which will be a clear end of communication and it is possible that important data get leaked. Thus, Privacy basically split into two brackets: Context Privacy and Data Privacy (Yao et al., 2013). These two categories include identity privacy, location privacy, timing privacy and data query, data aggregation respectively. The main concerns of privacy are to provide the Un-observability, Un-tractability, Un-linkability and Anonymity to the user.

Objective

The general objective of this study is to improve communication level between all sensor nodes and to decrease the transmission time along with preservation of location privacy of the node. "Random Walk" maintains the privacy of the present nodes in the network. Based on these enhancements, this research paper has three goals:

- To raise a safe communication network.
- To develop a scheme to provide privacy to the sensor and user nodes.
- To provide security in order to protect public safety and individual privacy.