Internet of Things : Secure-Key Management Protocols for Wireless Sensor Networks

Dhandapani Kothandaraman[1, a)] and Dr. Kadapa Sagar[2]

[1] *Sumathi Reddy Institute of Technology for Women, Warangal, Telangana, India.*
[2]*Professor, Dept. of CSE, CBIT, Hyderabad, Telangana, India*

[a)] Corresponding author: kothandaraman112@gmail.com

Abstract: The Internet of Things (IoT) aims to connect massive sensing devices through wireless networks to realize information interaction between the physical world and the virtual world. Wireless sensor networks, which have emerged as a result of advancements in wireless communication, micro electro-mechanical systems technology, and electronics, offer a wide range of future applications. In many circumstances, appropriate key management is required for networking security. The mechanism used to tackle the challenge of creating, establishing, distributing, and maintaining secret session keys is known as key management. Authentication and key exchange in IoT faces major challenges owing in part to the fact that constituent devices are resource constrained, deployed in environments where physical access to devices is possible. We describe ideas and strategies for designing authenticated key management systems for wireless sensor networks in an IoT environment. In this paper, we address several aspects related to pairwise key management, group key and establishment including issues related to authentication in existing literature. We also discussed literature on the design and implementation of lightweight group key management protocols that can be deployed in various IoT group applications along with research directions.

Keywords: Internet of Things, Wireless Sensor Networks, Security, Authentication, Key Management, Group Key management

INTRODUCTION

Nowadays, in the digital arena including the Internet of Things, Cloud Computing, spread of smart devices to multiple applications, smart grid systems, daily huge amount of data generated from heterogeneous sources such as health organisations, government, internet sources, social networks, and financial sectors [1, 2, 3]. WSN's include gigantic no of centers in a self-facilitated manner, where there are no central control center points, and the center points lying out of the sending reach can bestow in a multi-bounce way. IoT has turned into an incredible constituent cutting edge organizing advancements. In an IoT-empowered climate, things or actual items don't really remain inert. All things considered, they are linked to the Internet and equipped with handling and communication capabilities. Sensor networks are a critical building block of the Internet of Things. As a later turn of events, the Internet of Things (IoT) coordinates organized sensors like WSNs and, more as a rule, actual articles (i.e., things) in a pervasive the internet by interconnecting these frameworks to the Internet at large, making them additionally accessible over the web. Securing the group key establishment [14] in these multicast groups, it is critical that the message transmissions be given the legitimacy, validity, and privacy that they deserve [2]. Aside from these features, Cluster key foundation conventions must support IoT-enabled WSN properties such as asset needs, adaptability, and dynamic grouping.

A. Wireless Networks

WSN comprises of little sensors and utilized even in ignored climate, for example, sea-going area, terrestrial region, forest region and so on [1,19]. These sensors are low in their expense, memory and correspondence abilities. To work with secure correspondence, the sensors in WSN ought to secretly communicate their information starting with one sensor then onto the next or to the Base Station (BS). The credits of distant sensor networks choose the association security risks, the security structures, and security estimations that are extremely not as old as in standard associations [3], and the ordinary association security systems and security computations can't be introduced clearly.