Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 78 (2016) 579 – 586

Procedia Computer Science

International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, INDIA

Mathematical Model of Security Framework for Routing Layer Protocol in Wireless Sensor Networks

Ganesh R. Pathak[a], Suhas H. Patil[b]

[a]*Dept. of Computer Science and Engineering, Sathyabama University, Jeppiaar Nagar, Rajiv Gandhi Road, Chennai-600119, Tamil Nadu, India,*
[b]*Dept. of Computer Engineering, Bharati Vidyapeeth University College of Engineering, Pune-411043, Maharashtra, India*

Abstract

Most of the environmental and non-attended applications of Wireless Sensor Networks (WSN's) need mobile sensor nodes. However, mobility of sensor nodes increases security issues in WSNs and it's also vulnerable to various kinds of attacks. Dynamic WSN emerges two most common issues related to the authentication of moving sensor nodes and security in communication and key distribution. After possible movement of sensor node requires authenticating again and again from the base station or some other trusted nodes. Similarly, confidentiality in communication and key distribution is an important factoragainst man-in-middle type of attacks. Till the day most of the WSN's security researchers concentrate on the static environment. Though there schemes are secure and efficient but not sufficient to secure mobile WSN's environment. In this paper we have proposed a novel protocol framework and related mathematical model for secure routing layer communication and key distribution in mobile WSN's. After that we apply this model for performance evaluation on the basis of static as well as dynamic scenario for different number of nodes which shows that our framework is satisfactorily suitable for dynamic WSNs applications.

Peer-review under responsibility of organizing committee of the ICISP2015

Keywords:Wireless Sensor Networks; authentication; key distribution; mobility; Message Authentication Code

1. Introduction

WSN's domain has gained more popularity in research field. The reason behind this popularity is not only due to its applications but due to its co-domain fields also such as security, authentication, key management, routing, data aggregation, and disseminations etc.[10].

Basically WSNs consist of heterogeneous[4, 5] type of small devices that is sensor nodes those having small size, less memory[6, 9], limited battery power like properties along with the sensing capabilities. Sensor nodes can sense its

Peer-review under responsibility of organizing committee of the ICISP2015
doi:10.1016/j.procs.2016.02.121

surrounding environment to collect information related to the events happening in its range and based on some set of rules they disseminate that information to the base station via a wireless medium.

Most of the WSN's researcher's focuses on static sensor nodes which need one time authentication in WSNs. However dealing with mobile sensor nodes can pose different types of challenges and security related issues. Challenges are nothing but mobile node increases data transmission failure rate due to continuous route change in the network as well as increase in packet delivery delay which leads to bad affect in real time applications. Similarly, security related issues[7] like mobile nodes need authentication and re-authentication due to change in region as well as they are very prone to various types of both active and passive attacks by attackers or intruders also.

Whenever a mobile sensor node (slave node) connects to the WSN then sink node (master node) has to authenticate that slave node. In case mobile node moves to the range of another master node, master node needs to authenticate that slave node again. Hence, in high mobility environment master nodes need to authenticate slave nodes again and again though it had authenticated before by any other master nodes in the same network. Similarly, for node to node communication privacy plays an important role because intruders can tamper in between communication and make damage by changing information. Dissemination of authenticated key in WSNs is one of the basic security problems. As sensor nodes are light-weight devices and have limited memory and limited computational power[9], making the use of security protocols of other computer networks to WSNs is not enough. As a result, the primary issues in security researches on WSN are the design of resource-efficient security protocol. A number of approaches such as pre-distribution and hierarchical key management schemes, pair-wise key agreement and group based key agreement were introduced for the efficient authenticated key distribution[1, 2, 8]. So that our main goals are to reduce the load of frequent authentication, increase confidentiality and provide key freshness framework.

This paper is organized into five sections. The previous section covers the Introduction. Next section describes the proposed protocol description. Section 3 explains actual mathematical model of proposed protocol framework for secure routing layer protocol. Section 4 describes performance evaluation and the final section concluded the paper.

2. SRL protocol description

In this section we have described our proposed protocol framework for secure routing layer communication and key distribution in dynamic WSNs. Figure 1 show the block diagram of our proposed protocol which consists of base station (BS), two master nodes (S1, S2) and a slave node (N). This framework is divided into five stages viz.

a. Stage 0: Determination and Discovery of Master Nodes.
b. Stage 1: Master Nodes Communication Set-up.
c. Stage 2: Master Nodes Distribution of Authentication Keys.
d. Stage 3: Primary Authentication of Slave Nodes.
e. Stage 4: Secondary Authentication of Slave Nodes.