Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 125 (2018) 201–207

Procedia Computer Science

www.elsevier.com/locate/procedia

6th International Conference on Smart Computing and Communications, ICSCC 2017, 7-8 December 2017, Kurukshetra, India

An attack model based highly secure key management scheme for wireless sensor networks

Priyanka Ahlawat*, Mayank Dave

Department of Computer Engineering
National Institute of Technology, Kurukshetra Haryana

Abstract

Wireless sensor network (WSN) security is a critical issue due to its inherent characteristic and unattended operation which makes it vulnerable to many attacks. Key management plays a fundamental role for providing security services to such networks. In this paper, we aim to reduce the node capture impact by incorporating an efficient adversarial model for cellular model of WSN. The adversarial model exploits several vulnerabilities present in the network such as high node density, placement of the sink node, neighbour influence factor to compute the compromise probability of each cell. It then defines the hash chain length for each cell with different rekey interval to increase the network resistance against node capture attack. The proposed scheme is compared with other existing schemes in terms of the probability of key compromise and the number of links rekeyed. The results confirm its effectiveness in increasing the WSN security.

Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications.

Keywords: Wireless sensor network; Rekeying; Key management scheme; Attack model; Node capture attack

* Corresponding author. Tel.: 01744233479 fax: +0-000-000-0000 .
E-mail address: priyankaahlawat@nitkkr.ac.in, mannpammy@gmail.com

1877-0509
Peer-review under responsibility of the scientific committee of the 6th International Conference on Smart Computing and Communications
10.1016/j.procs.2017.12.028

1. Introduction

Wireless Sensor Networks (WSN) are composed of small, resource constrained sensors placed in hostile environments, thus are very susceptible towards node capture attacks. In such attacks, adversary captures the node and steal the secret keying information from it. Thus, to provide secure communication even in presence of adversary is a challenge in WSN security[1]. Key management scheme (KMS) plays a very fundamental role in providing security to networks. It is defined as a set of mechanism that support any ongoing communication between valid nodes. These sensors find enormous applications in the areas of battlefields, wild life monitoring, fire detection, medical applications like patient monitoring and tracking, smart environments, traffic surveillance, flood detection etc.[2] In this paper, a highly secure key management scheme based on efficient adversarial model is proposed. Attacker is assumed to be intelligent and tend to capture minimum number of nodes to destroy the complete network traffic. In the proposed scheme, compromise probability of each cell is computed and then, a hash chain is created based on it [3]. We aim to assign the hash chain length of a cell based on the security requirement of that network.

This paper is organized as follows: In Sect. 2, we briefly discuss the related existing key predistribution schemes in WSNs. Sect. 3 discusses proposed scheme. The performance analysis of the proposed scheme with other schemes is presented in Sect. 4. Finally, we conclude the paper in Sect. 5.

2. Background Study

A number of KMSs are proposed in the literature for WSN. It plays a very important role in providing confidentiality, integrity of ongoing communication between the nodes. The earliest scheme was proposed by Eschenaur and Gligor for homogenous networks [4]. In this scheme, key distribution server (KDS) assigns equal number of keys to every node in the network. Neighboring nodes can only communicate when they have at least one common key in their key ring. It was further enhanced by Chan et al where instead of sharing one key, nodes share at least q keys to establish a secure connection [5]. Du et al. [6] presented a deployment based KMS where the adjoining nodes share more keys than other non adjacent nodes. Requirement of prior deployment knowledge limits its use in many practical applications. Hash based mechanisms are used in [7-11] to enhance the security of the network. Authors in [7] applied hashing based on node identifiers value. It is shown that it has improved performance in terms of resilience against node capture, computation overhead and communication overhead. A scheme with two hash functions is presented in [8] in which a 2 dimensional hash chain is produced to increase its security. A large number of adversarial models are presented in [12-21]. These are broadly classified as system theoretic analysis, epidemic theory, probability analysis method, vulnerability evaluation method and graph theory. These models assume that adversary is intelligent and has bounded potential. Attack model using sink as a factor are given in [20-21]. A rekeying approach is discussed in [22]. A hybrid KMS is presented in [23] to increase the security of KMS. A matrix based attack modeling is presented in [24-25] to increase the destructiveness of attacker.

So far, most of key management schemes are designed independent of underlying attack model. Thus, these schemes may fail in some real time applications. Even the hash based mechanism are applied without considering any attacking behavior of the adversary. The attacking pattern can be effectively used to design various counteracts in WSNs. The proposed matrix based attack model enhances the defender capability to defend against attacks before their occurrence in the system. In conclusion, there is a need to design the key management schemes according to actual security requirements. We also observe that different attack models, hash mechanisms can be effectively combined to design attack resistant KMS for WSNs.

3. An attack model based highly secure key management scheme for WSN

The attacker aims to destroy the confidentiality and integrity of the network by capturing of the nodes. In the proposed scheme, before pre-distributing the keys in the nodes, a matrix based attack model is constructed and compromise probability of every cell is then computed. The whole pool of keys is divided in to m sub key pools where m is the total number of cells. A 2-D hash chain is then created based on the compromise probability of each cell[8]. Each node of same cell is assumed to have same compromise probability. In shared key discovery, the nodes