Journal of King Saud University – Computer and Information Sciences xxx (2018) xxx–xxx

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

An attack resistant key predistribution scheme for wireless sensor networks

Priyanka Ahlawat *, Mayank Dave

Dept. of Computer Engineering, National Institute of Technology, Kurukshetra, Haryana, India

ARTICLE INFO

Article history:
Received 11 October 2017
Revised 12 February 2018
Accepted 3 March 2018
Available online xxxx

Keywords:
Attack probability
q-Composite scheme
Resilience against node capture
Key connectivity
Random key predistribution scheme

ABSTRACT

Most of the key management schemes do not consider the attacking behavior of the adversary making such schemes less practical in real world. By knowing the adversarial behavior, several countermeasures against them can be effectively and efficiently designed by the defender/network designer. In this paper, we investigate the problem of node capture attack and propose a secure hybrid key predistribution scheme (HKP-HD) for wireless sensor networks (WSN). This scheme combines the robustness of the *q*-composite scheme with threshold resistant polynomial scheme. The proposed scheme aims to make the network more resistant against the node capture attacks. Adversary is assumed to be intelligent that tends to exploit different vulnerabilities present in network to build an attack matrix. It aims to destroy complete network with least number of nodes based on the attack matrix. As a countermeasure, the network designer constructs similar attack matrix based on the vulnerabilities in the network by considering sink as a major influencing factor. This matrix is used to calculate the attack coefficient of every node of the network that determines its probability of attack by the adversary. A hash chain based on maximum value of attack coefficient along with the multiple key pools is used to reduce the probability of the key compromise and communication overhead of the proposed scheme. The simulation results demonstrate that the proposed scheme has reduced probability of key compromise, communication overhead and storage overhead as compared to other schemes.

1. Introduction

Wireless sensor network (WSN) comprises of small resource constrained sensors that actively monitor their surroundings, collect the data and send it to the central authority. The central authority is the base station (BS) that acts as a powerful data processing and storage center (Aikyildiz et al. 2002). The sensors have limited energy and processing power that makes the heavy weight public key encryption infeasible solution for WSN security. The security mechanisms should be lightweight and energy efficient for WSN. Duty cycled WSNs in which sensor are sleep and awake at some interval of time is one such technique to reduce the energy consumption during query processing (Zhu et al., 2015a,b). Location based sleep scheduling is another technique to improve the energy efficiency of WSN integrated with mobile cloud computing (Zhu et al., 2015a,b). As the sensors have limited resources and deployed in the hostile environments, WSNs are susceptible to various attacks. One such attack is the node capture attack. The resistance of key management scheme (KMS) against this attack emerges an important and challenging issue in WSN security. The WSN security resides in securing the keys used for encrypting the data (Zhang and Varadharaja, 2010; Bhushan and Sahoo, 2017). Therefore, the fundamental question is how to design a secure a KMS that guarantees the proper functionality of WSN services even in the presence of the adversary (Eschenauer and Gligor, 2002). WSNs have applications in diverse domains such as defense, medical care, environmental monitoring, disaster management, inventory control etc. KMS is the set of processes that facilitate the secure transmission of data between sensor nodes (Chan et al. 2003; Choi et al. 2017; Ling et al. 2008).

1.1. Research motivation

Due to wireless nature of communication channel, there are many inherent security issues such as eavesdropping, forgery

* Corresponding author.
E-mail addresses: priyankaahlawat@nitkkr.ac.in (P. Ahlawat), mdave@nitkkr.ac.in (M. Dave).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2018.03.002
1319-1578/

Please cite this article in press as: Ahlawat, P., Dave, M. An attack resistant key predistribution scheme for wireless sensor networks. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.03.002

attacks, off-line guessing attacks etc in WSN. These networks are often deployed in unattended, hostile and critical environments, thus there is a need for effective and efficient techniques to fulfill the security requirements. Key establishment schemes aim to provide pair-wise keys among the neighboring nodes to support ongoing relationship in a network. But it becomes complicated due to the limited computational power, battery power and storage capacity of sensor nodes. Most of the KMS assumes that every node of the network has same probability of attack. This assumption may not be true for many WSN applications such as military and border surveillance making these schemes less practical in real world environments. Can we develop mechanisms that both resilience and connectivity of key predistribution schemes increases? It was also pointed that "a system without adversary definition cannot be secure. It can only be astonishing" by Gligor (2008). It states that defensive mechanisms should be designed after analyzing the adversary behavior. Had there been a reliable, secure and realistic designed KMS for WSNs, an attack such as node capture would not be able to degrade the performance of KMS to such an extent. Motivated by this fact, this paper presents an attack resistant key predistribution that combines the strong points of the q-composite with the polynomial scheme to make the network more secure against node capture. Further, the communication overhead is reduced by introducing multiple key pools in the predistribution of the proposed scheme. The paper aims to improve the security and communication overhead of the KMS without degrading its performance (Bechkit et al., 2013; Du et al., 2007; Zhang et al., 2016a,b; Mohaisen et al., 2010; Mary et al., 2015)

1.2. Research contributions

The main contributions of the proposed paper can be summarized as under:

(i) The paper formalizes the probability of capturing of a node in terms of its attack coefficient. It is based on several vulnerabilities present in the network that can be easily exploited by the adversary to destroy the network.
(ii) We have combined q-composite scheme with the polynomial pool scheme. to increase the resilience against node capture attack of the proposed scheme.
(iii) The concept of unbalanced key distribution with multiple sub key pools is utilized to pre-distribute the keys in the sensor nodes. A small key ring size is assigned to the vulnerable nodes and large key ring to the safe nodes. It increases the resistance against node capture and reduces the communication overhead of the proposed scheme.
(iv) An attack coefficient based hash chaining is performed in the pre-distribution phase of the proposed scheme. This reduces the probability of key compromise of the proposed scheme.

1.3. Organization of the paper

The article is structured as follows: Section 2 introduces the related key management schemes for WSNs. Section 4 introduces the various system models used in proposed scheme. Section 4 presents the proposed scheme HKP-HD. A case study to demonstrate the effectiveness of the proposed scheme is given in Section 5. The analysis of the proposed scheme is done in Section 6 followed by comparative analysis with other existing schemes in Section 7. Finally, Section 8 concludes the paper.

2. Literature survey

Due to their inherent properties, WSNs are susceptible to various attacks. These attacks break the confidentiality, integrity and availability of the network. Such attacks can be classified as passive and active attacks. The listening of communication channels by unauthorized users is the passive attacks such as eavesdropping, traffic analysis and passive monitoring. These attacks breach the confidentiality and privacy of the network data. The active attacks falsify, modify, listen, monitor the data packets in the network. The common active attacks are camouflage, sybil, wormhole, replay, hello flood, sink hole, denial of service, and node replication. Sink is the most trusted component of the WSN and cannot be compromised by the adversary. It acts as a gateway to forward the collected data to some external environment and thus, sink hole node detection becomes an important in WSN security (Wazid et al., 2016). Even some attacks such as black hole are difficult to detect and defend and thus, their timely detection and prevention is crucial in the network security (Wazid and Das, 2017). Authentication also is an important aspect of security as it allows the authorized access to information available through sensor nodes (Wu et al., 2016). The security requirements along with their possible solutions are listed in Table 1.

In this paper, we focus on the key distribution schemes in WSN security. KMS plays a very significant role by establishing secure communication among the sensor nodes. In 2002, Eschenauer and Gligor (2002) proposed random key predistribution scheme for WSNs. This scheme is also called EG scheme or the basic scheme. It has three phases - key predistribution, discovery of shared key and establishment of path key. The keys are assigned from a large key pool. If the nodes are not able to find a common key, they perform path key establishment with intermediate nodes. EG scheme was further strengthened by the q-composite scheme where the nodes have to share q keys instead of one key (Chan et al., 2003). This increases safety of the scheme. Deployment based key management scheme is given Du et al. (2004) in which the neighboring nodes share more number of keys than non neighboring nodes in a network. The requirement of prior deployment information limits the practical use of such schemes. Authors Choi et al. (2017) present a secure scheme by considering threats that may occur inside the network. A polynomial pool scheme is proposed (Ling et al., 2008) that uses bivariate polynomials to establish the pair-wise key. This scheme suffers from large storage overhead but has high security in small scale attacks. The polynomial scheme has t-threshold property which states that the scheme is not compromised if the number of captured nodes is less than t. In recent researches, many scholars have presented a combined approach that combines the advantages of two different schemes with limited complexity. Authors Bechkit et al. (2013) presented a hash based key pre-distribution scheme for WSN. The hash function is used to conceal the pre-distributed keys from an adversary. It is shown that this scheme has increased resistance against node capture. An unbalanced key distribution scheme is proposed in Du et al. (2007) that assign larger key ring size to high end sensors and minimum key ring size to low end sensors. This increases the overall performance of KMS. A scheme called PPBR that combines polynomial and random key predistribution is

Table 1
Security requirements in WSN security and their possible solutions.

Goals in WSN security	Possible solutions
Confidentiality	Encryption schemes, access control schemes
Integrity	Digital signature, hash function
Availability	Intrusion detection system, authentication schemes
Access control and authorization	Access control schemes, key distribution schemes, encryption schemes
Authentication	Random key distribution, digital signature
Forward and backward secrecy	Key distribution schemes

Please cite this article in press as: Ahlawat, P., Dave, M. An attack resistant key predistribution scheme for wireless sensor networks. Journal of King Saud University – Computer and Information Sciences (2018), https://doi.org/10.1016/j.jksuci.2018.03.002