Ad Hoc Networks 37 (2016) 324–336

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance in wireless sensor networks

Xinjiang Sun[a], Xiaobei Wu[a,*], Cheng Huang[a], Zhiliang Xu[a], Jianlin Zhong[a,b]

[a] School of Automation, Nanjing University of Science and Technology, Nanjing 210094, PR China
[b] Shanghai Key Laboratory of Multiphase Flow and Heat Transfer in Power Engineering, Shanghai 200093, PR China

ARTICLE INFO

Article history:
Received 20 January 2015
Revised 19 July 2015
Accepted 20 August 2015
Available online 9 September 2015

Keywords:
Wireless sensor networks
Self-healing key management
Access polynomial
Sliding window
Broadcast authentication
Collusion resistance

ABSTRACT

Though lots of research results about self-healing key management under unreliable links have been proposed, there are still some shortcomings, such as the inefficiency of broadcasts, lack of broadcast authentication, limited sessions for key issues, disastrous risks of access polynomials, and the vulnerability of collusion attacks. In this paper, we propose two modified access polynomial based self-healing key management schemes with broadcast authentication and enhanced collusion resistance. First, two kinds of attacks are introduced to break the security of access polynomials. Then, a modified security model is given, and collusion resistance capability is redefined from the perspective of session interval from node revocation to node addition, which does not depend on the number of collusive nodes. Next, based on sliding window and modified access polynomial, *Sch-I* and *Sch-II* are proposed to achieve the security and tolerate packet losses, which allow pairwise keys between member nodes and group manager to be updated dynamically. Finally, theoretical analysis validates that the proposed schemes have δ self-healing capability, *any*-wise forward security and backward security, and enhanced collusion resistance capability, and can also avoid the flaws of access polynomials and reduce the resource consumption. Compared with existing schemes, they are quite suitable for practical applications.

1. Introduction

During the last decades, various applications have been benefitting from wireless sensor networks (WSNs), such as environmental monitoring, battlefield intelligence and reconnaissance, medical caring, intelligent home, industrial control, etc. [1]. However, in some harsh and critical environments, malicious attacks, including eavesdropping, DOS attacks, and packet tampering and infection, may disturb the network operations and degrade the network performance. Security issues should be considered carefully during the design of WSNs' protocols to defense and tolerate these attacks [2]. Cryptography is typically used to provide the security, such as confidentiality, authentication, integrity, and availability [3]. As the core role of the security, key management is responsible for key distribution, updating and revocation for sensor nodes, and establishes security associations between sensor nodes [4,5].

Due to the dynamic topologies, node mobility and interferences caused by environment noises or human, wireless links may change temporally and spatially, leading to random packet errors or losses. Consequently, the loss of the messages for key issues will make security keys asynchronous and security associations failed. Traditional methods to

* Corresponding author. Tel.: +86 189 5179 1810; fax: +86 025 8431-6158.
E-mail addresses: xinjiangsun@gmail.com (X. Sun), wuxb@njust.edu.cn, sxj_njust@163.com (X. Wu), hearthc@163.com (C. Huang), zhlxunjust@163.com (Z. Xu), njustzhongjianlin@163.com (J. Zhong).

http://dx.doi.org/10.1016/j.adhoc.2015.08.027
1570-8705/

recover lost keys for each node, such as retransmissions, are inefficient. In 2002, Staddon et al. in [6] first addressed the problem of self-healing key management, and since then a lot of research results have been carried out [7]. In self-healing mechanisms, some redundant information should be added in the broadcast message, which enables nodes to recover lost session keys independently and non-interactively [7]. With the help of self-healing mechanisms, network transmissions and workloads of group managers can be greatly reduced, and the risk of network traffic analysis by attackers may also be minimized.

In accordance with mathematical methods used, the related researches include polynomials [6,8], vector space secret sharing [9], bilinear pairings [10] and elliptic curve cryptography [11], etc. Since some features of polynomials can be utilized to make a better trade-off between security performances, computation complexity and resource consumptions artfully than other methods [7], we focus on polynomial based schemes in this paper to achieve better network performances. The polynomials used for self-healing mechanisms can be classified into three categories: secret sharing polynomial, revocation polynomial and access polynomial. (1) Staddon et al. in [6] first proposed some schemes based on secret sharing polynomial, which only resists *t*-revocation and can be broken by the Lagrange Interpolation method easily. Blundo et al. in [12] gave novel univariate polynomial based schemes, and an exponential algebraic method to handle the polynomial reuse problem, which also exists in [6] before. However, the backward security is lost. A modified exponential algebraic method was given in [13] to support long-lived group key distribution scheme with backward secrecy. The computation overheads of exponential algebraic methods are still too high to fit resource-constrained wireless networks. (2) Revocation polynomial was first proposed by Liu et al. in [14] and simplified by Hong et al. in [15], which further reduces the storage and communication overhead. Then, there appeared many related schemes based on revocation polynomial [8,16–19]. However, some security flaws still exist, which are already analyzed in [20,21], and the communication overhead will increase with the number of revoked nodes. (3) Access polynomial was first proposed by Zou et al. in [22,23] to restrict that only legitimate nodes can get the keys using their access information, which reduces the communication and storage overhead. Then, several schemes are proposed in [24–29] to improve the security. However, there still exist some flaws. Due to the inappropriate random factor used, the scheme in [26] has fatal flaws that attackers can break the security, seen in Section 3.2. Wang et al. in [27] gave a modified mechanism, which has the enhanced security, but its communication overhead is still high. In addition, it was pointed out in [30] that the forward and backward security could not be guaranteed in the scheme [28]. Moreover, nearly all access polynomial based schemes [22,24–29] are vulnerable to a disastrous attack called Polynomial Factorization [31–33], which makes the roots of access polynomials and even the secret information exposed to attackers easily, seen in Section 3.3.

On the other hand, the methods for constructing redundant information in self-healing mechanisms can be classified into two kinds: related approaches and independent approaches. (1) In the related approaches, one session key and the relationship between different session keys are contained in the broadcast message to recover lost keys, where the forward and backward hash chains are mostly adopted. Thus, the communication overhead can be further reduced, but some security problems arise, such as weak collusion resistance in [9,17,26,27,34], the restriction that nodes cannot be revoked during their lifetime in [16,18,35] and only supporting limited sessions for key issues in [34,36,37]. (2) Independent session key means that no mathematical relationship exists between each key. Lost keys can be recovered from single message in [8–10,12,17,18,24,26,27,34–37] and two or more messages in [6,8]. Compared with related self-healing schemes, independent schemes have much more flexibility, and higher communication overheads. Sliding window proposed in [38] can help reduce communication overheads. Additionally, almost existing schemes can only achieve *t*-wise or *mt*-wise collusion resistance, but not *any*-wise collusion resistance.

In order to alleviate the problems existing in pioneers' research, we propose two self-healing key management schemes based on modified access polynomial and sliding window in WSNs. The main contributions of this paper are given as follows.

(1) Based on the unconditional security in information theory, a novel self-healing security model is given, where several security performances are quantified from the perspective of system parameters, such as the capability of self-healing and collusion resistance. Particularly, collusion resistance capability is redefined from the perspective of session interval from node revocation to node addition.
(2) Flaws of the schemes based on access polynomial are pointed out. We introduce the *PEK-attack* to break the forward and backward security in [26]. In addition, the important and disastrous strategy, polynomial factorization attack (*PF-attack*), is introduced to break the security of access polynomials. Then, an effective mechanism is proposed to tolerate *PF-attack* and packet losses as well.
(3) Two novel self-healing key management schemes: *Sch-I* and *II* are proposed. *Sch-I* introduces an idea that the pairwise keys shared between member nodes and group manager are updated dynamically, which declines the vulnerability of access polynomial. The one-way hash chain guarantees the forward security; the modified access polynomial provides the backward security; and the sliding window mechanism reduces communication overhead. *Sch-II* only removes the hash chain but can strengthen the security.
(4) Two proposed schemes are analyzed in terms of the security, efficiency and flexibility. Our schemes have *any*-wise forward and backward security, self-healing capability and enhanced collusion resistance. And they can also avoid the flaws of access polynomials, support infinite sessions for key issues, adaptive configurability, and reduce resources consumption. Additionally, they support broadcast authentication and integrity protection, which has drawn few or no attention from the existing schemes. Compared with existing schemes, the schemes