Computers and Electrical Engineering 48 (2015) 405–416

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Reliable anonymous secure packet forwarding scheme for wireless sensor networks ☆

S.V. Annlin Jeba [a,*], R. Suresh Kumar [b]

[a] Department of Computer Science & Engineering, C.S.I. Institute of Technology, Tamil Nadu, India
[b] Department of Mathematics, C.S.I. Institute of Technology, Tamil Nadu, India

ARTICLE INFO

Article history:
Received 19 July 2014
Received in revised form 26 August 2015
Accepted 28 August 2015

Keywords:
Anonymity
Identity
Optimal route
Communication
Link quality
Security

ABSTRACT

Designing a lightweight, secure communication protocol for Wireless Sensor Networks (WSNs) remains a challenging issue since sensor networks are resource limited and are left unattended. Sensor nodes in WSNs are subjected to varying forms of attacks. An adversary may destroy or damage the communications done in multi-hop WSNs by means of packet dropping and modification. Hence it is essential to have an efficient cryptographic scheme to protect the communications done in WSNs. This study introduces a Reliable Anonymous Secure Packet forwarding (RASP) scheme that can prevent not only traffic analysis attack but also the attacks done through compromised forwarding nodes. The mechanisms followed here are effective with low computation and communication overhead. The performance of the proposed scheme is evaluated over NS2 with a series of simulation. The simulated results show that the proposed scheme performs better than other comparable schemes.

1. Introduction

Rapidly developed WSN technology is widely used in different types of applications due to its economic and viable nature. A WSN is composed of a large number of sensor nodes which are connected through wireless links. The sensor nodes send data to Base Station (BS) through multi-hop transmission. The Wireless nature of communication, resource limitation on sensor nodes and unknown network topology prior to deployment makes the sensor nodes vulnerable to various security attacks [1,2]. From the security standpoint it is essential to provide authentic and accurate data to the BS. Previous security schemes focus on security services such as authenticity, confidentiality and integrity [3]. In addition to these services, many applications of WSNs have special requirements in terms of privacy and security [4,5].

Different key management schemes [6–8] have been developed to ensure data security in different circumstances for WSNs. Security relevant issues in WSNs and the issue of key establishment are considered in this literature [6]. Key predistribution through public key cryptography has been demonstrated in [7]. Energy limitation of sensor nodes make the use of public key systems impractical for WSNs. Security in hierarchical WSNs can be achieved using combinatorial designs [8,9]. This scheme assigns key chains to sensor nodes before deployment which reduces communication overhead. However, it requires more key space and it is not an energy efficient mechanism. To overcome these issues full pairwise key management

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. M.H. Rehmani.

* Corresponding author.
E-mail addresses: annlin_jeba@yahoo.co.in (S.V. Annlin Jeba), sureshannlin@gmail.com (R. Suresh Kumar).

http://dx.doi.org/10.1016/j.compeleceng.2015.08.021
0045-7906/

scheme can be adopted [10]. This is achieved by sharing pairwise key between neighbouring nodes. In a WSN with '*n*' nodes each node desires its key to be predistributed with $n-1$ nodes [11]. This scheme causes storage of large number of keys in each node. Moreover, maintaining forward and backward secrecy through this scheme is also a challenging task. If a node is compromised all the secure links connecting the compromised node with other nodes get affected. To reduce the node compromisation probability random key predistribution scheme can be followed. In random key predistribution process each node is assigned with a ring of keys selected randomly from a key pool [11]. But when a node is compromised all its keys and all the links secured by these keys are also compromised.

Recently many approaches have been proposed for providing hop-by-hop authentication [12]. These mechanisms need to share pairwise key between consecutive neighbouring nodes along with the selected path. But these schemes may function efficiently if all the links in the network are highly resilient to compromisation. [13].The proposed RASP mechanism considers security and privacy as important concern in packet forwarding. Further, it avoids unauthorised and infected traffic from being forwarded to the next hop. Simulation results and analytical studies verify the achievability of the proposed scheme.

1.1. Contributions

The key contributions of the proposed scheme are as follows:

- This scheme ensures reliability in communication by selecting optimal forwarding nodes which avoids frequent failure of nodes along with the selected path.
- It preserves the privacy of the sensor nodes involved in communication through the security service anonymity. This feature prevents the occurrence of traffic analysis attack.
- Incremental hash based authentication technique is followed in this scheme which allows immediate authentication of the packets received. This mechanism prevents compromised data from being forwarded in the network.

1.2. Notation

For the reason of clarity, the notations used throughout this study are listed in Table1.

The rest part of the paper is organised as follows. Some literatures related to the proposed scheme are discussed in Section 2. Section 3 presents the detailed description of the proposed scheme, followed by analysis and discussion in Section 4. Analysis through simulation is presented in section 5. The proposed mechanism is concluded in Section 6.

2. Related works

Recently, many secure communication schemes have been investigated by researchers to resist the vulnerabilities caused in WSNs. Some of the related schemes and their security relevant issues have been presented in this section. Literature

Table 1
Notations.

Notations	Descriptions
S_{ID}	Source identity
H()	Hash function
Enc $_{SID}$	Encryption using source identity
Pkt_info	Encrypted message in the packet
Auth_info	Authentication information
REQ	Format of request message
BS_{ID}	Base station identity
Hop_{ID}	Identity of the next hop or forwarding node
XOR	Exclusive OR
Dec_{SID}	Decryption using S_{ID}
REP	Format of the reply message
SK	Secret key
SD	Secured data
RS	Random string
Enc $_{SK}$	Encryption using secret key
t_w	Time window
RE_{thres}	Threshold value for residual energy
T_{source}	Time consumed by source to generate report
T_{hop}	Time consumed by forwarding node
T_{BS}	Time consumed by base station
T_{Hash}	Time to perform single hash operation
T_{XOR}	Time to perform single exclusive OR operation
T_{Rand}	Time for random selection of 128 bits
T_{Dec}	Time to decrypt a message
T_{Enc}	Time to encrypt a message
||	Concatenation operator