Computers and Electrical Engineering 44 (2015) 172–183

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A new three party key establishment scheme: Applicable for internet-enabled sensor networks ☆,☆☆

Hassan Nasiraee *, Jamshid B. Mohasefi

Department of Computer Science and Engineering, Urmia University, Urmia, Iran

ARTICLE INFO

Article history:
Received 27 January 2014
Received in revised form 28 September 2014
Accepted 2 October 2014
Available online 15 November 2014

Keywords:
Security
Three party key establishment
DoS attacks
Sybil attack
Internet-of-Things
Internet-enabled sensor networks

ABSTRACT

Internet-Enabled Sensor Networks (IESNs) play an important role in Internet-of-Things (IoT) which usually need key establishment and secure communication. In this paper, first we show why existing three party key establishment schemes cannot be easily applied to IESN. Second we propose an extension of traditional three-party key establishment schemes (such as SNEP, BBF and OR). The method provides DoS and Sybil attack resistance and benefits from low communication cost, independence of prior sensor deployment knowledge and support for node mobility. The extension is simple in the sense that an interested node that joins the network is responsible to aggregate neighbors' information and to send a request to the trusted party to get required keys. Our proposal reduces energy consumption about 75% vs. SNEP, 50% vs. BBF and 78% vs. OR, as three well-known previous schemes, which causes a significant increase in lifetime of nodes.

1. Introduction

In the next decade, the traditional networks and the Internet network objects are expected to have an integrated structure. An Internet enabled WSN, known as IESN, is an important part of the IoT. IESNs, similar to WSNs, usually contain many small autonomous devices called sensor nodes. A sensor has constraints on resources such as energy, space and memory because of the constraints on size and cost. Sensor networks have many applications such as military, nuclear installations monitoring, civilian applications, monitoring habitat, temperature, motion, noise, seismic activity, health, and traffic management [1].

Many applications of sensor networks require secure communication. Thus establishing a secure channel between any two sensor-nodes in WSNs/IESNs is important for many applications, such as secure data exchange, secure data aggregation, and secure routing.

On the other hand, in comparison to other kinds of communication networks, WSNs are vulnerable against resource depletion attack on power and bandwidth due to their constraining properties. Moreover, sensor networks are vulnerable against various attacks such as identity theft, Sybil attack, fraud, masquerading, interception for misleading, because of

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Maurizio Palesi.

☆☆ This is a full version of a primarily paper presented at ISCISC 10th IEEE International ISC Conference on Information Security and Cryptology (ISCISC13), ISCISC, Yazd, Iran, September 2013.

* Corresponding author. Tel.: +98 441 2972880; fax: +98 441 2972837.
E-mail address: hnasir20@gmail.com (H. Nasiraee).

http://dx.doi.org/10.1016/j.compeleceng.2014.10.001

the wireless connectivity and lack of physical protection [2–5]. Thus, there is a need for a secure and efficient shared secret establishment among sensor nodes in IESNs as well as WSNs.

1.1. Motivations

The importance of key establishment schemes led to development of many schemes for traditional WSNs. They have their own advantages and disadvantages. The flexibility and node mobility are more required properties in IESN [6]. With the best of our knowledge, there is no any proposed key establishment scheme specific for IESN until now. In fact, in an IESN, we need a key establishment scheme, which does not need network deployment knowledge such as final position of nodes or any prior deployment knowledge. This can be provided using three party key establishment schemes. However, these schemes are assumed impractical for traditional WSNs, due to absence of trusted party and limitation of communication range in sensor nodes. Although, in IESN, trusted third party can be provide in the Internet. Our aim is to present a key establishment scheme for IESN, which satisfies essential security and efficiency metrics, such as DoS resistance, Sybil attack resistance and low communication overhead.

1.2. Our contributions

In this paper, first we show vulnerability of three existent traditional Internet style schemes against DoS (Denial-of-Service) attack in resource-constrained networks. Then we propose an efficient DoS and Sybil attack resistant three party scheme. In the proposed scheme, a mobile sensor node is able to establish secure channel with another node even if they are not met before. Since our proposal is an extension of three previous well-known schemes explained in the literature, in experimental results and implementation, we only discuss the effects of this extension over those three schemes. As a final contribution, we elaborate architecture for IESN and discuss the application of our extended scheme in this architecture.

1.3. Assumptions

We assume sensor nodes are mobile and may establish secure channels with other nodes, even with those, whom are not met before. An attacker can easily intercept, sniff, store, modify all the interchanged messages between nodes, and launch a resource depletion attack. An attacker is present before the network deployment and during the whole network lifetime.

1.4. Paper organization

The rest of this paper is organized as follows: In Section 2, we review the important metrics to design a key establishment scheme for IESN, and discuss four well-known and brilliant previous works. In Section 3, we introduce our key management scheme in details. In Section 4, we discuss security of our method. Section 5 is dedicated to energy consumption evaluation and comparisons with other methods. In Section 6, first, we describe a more probable architecture for IESN and then we describe application of our proposed method in this architecture. Finally, we conclude the paper in Section 7.

2. The requirements and previous works

In the following, we review some important requirements and discuss previous works.

2.1. The requirements

P1. *Lack of prior deployment knowledge and node mobility:* In sensor nodes enabled by the Internet and in many applications of traditional WSNs, the nodes are distributed dynamically and randomly. In a few situations (e.g., when the nodes are deployed by hand), it is possible to assume some degree of proximity between groups of nodes, at least in the early days of the network. Hence knowing final positions of nodes is difficult. In fact, in applications that use the nodes' location for their normal operation, such knowledge is usually gathered after deployment (e.g., using a built-in GPS). Therefore, more flexible key establishment techniques do not rely on the positions of nodes [4,5].

P2. *Node-to-node authentication:* As a definition, if a scheme provides node-to-node identity authentication, any node would be able to verify the identity of other nodes it is communicating with them. Moreover, an adversary is unable to impersonate other nodes unless they are captured already.

P3. *Resilience:* As a definition, a scheme obtains a perfect score (i.e. perfect resilience), when having a compromised node reveals no information about links that are not directly involved to that node.

P4. *Bit/signal transmission distance:* Since energy consumption grows with the forth power of magnitude of distance in sensor networks [4,5], minimizing data transmission to long distances is one of the key goals of designing an efficient scheme. As we show later, the lack of care about this performance metric leads to request-based DoS attacks which depletes power of nodes.

P5. *Key connectivity:* It is the probability that any two arbitrary nodes would be able to make a shared secret.