Ad Hoc Networks 20 (2014) 96–112

Contents lists available at ScienceDirect

Ad Hoc Networks

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

A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion

Muhamed Turkanović *, Boštjan Brumen, Marko Hölbl

University of Maribor, Faculty of Electrical Engineering and Computer Science, Maribor, Slovenia

ARTICLE INFO

Article history:
Received 19 June 2013
Received in revised form 23 December 2013
Accepted 31 March 2014
Available online 13 April 2014

Keywords:
Wireless sensor network
Ad hoc
Mutual authentication
Key agreement
Smart card
Internet of Things

ABSTRACT

The idea of the Internet of Things (IOT) notion is that everything within the global network is accessible and interconnected. As such Wireless Sensor Networks (WSN) play a vital role in such an environment, since they cover a wide application field. Such interconnection can be seen from the aspect of a remote user who can access a single desired sensor node from the WSN without the necessity of firstly connecting with a gateway node (GWN). This paper focuses on such an environment and proposes a novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks. The proposed scheme enables a remote user to securely negotiate a session key with a general sensor node, using a lightweight key agreement protocol. The proposed scheme ensures mutual authentication between the user, sensor node, and the gateway node (GWN), although the GWN is never contacted by the user. The proposed scheme has been adapted to the resource-constrained architecture of the WSN, thus it uses only simple hash and XOR computations. Our proposed scheme tackles these risks and the challenges posed by the IOT, by ensuring high security and performance features.

1. Introduction

We are evermore surrounded by ubiquitous, intelligent interconnected objects (i.e. smart objects) which engage us with new applicative perspectives on our everyday lives, like RFID, smartphones, semantic web, wireless sensors, etc. This can be seen as the Internet of Things (IOT) notion, which was announced a decade ago [1]. The idea was that in the future everything (i.e. including live objects) would be accessible, sensed, and interconnected inside the global, dynamic, living structure of the Internet. Wireless sensor networks (WSN) play an important role regarding this notion, since they cover a wide application field by collecting various environmental information.

In the early years WSNs started as simple and ambivalent research projects mainly motivated and funded by the military, e.g. DARPA (Defense Advanced Research Projects Agency) [2]. These early military-funded WSN research projects, according to their type of applications, presented a definition of the WSN as a large-scale, wireless, ad hoc, multi-hop, un-partitioned network of homogeneous, tiny, mostly immobile sensor nodes which are randomly deployed within a particular area of interest [2]. Such a definition does not apply to all of today's WSN applications, since WSN applications can also be heterogeneous, single-hop, infrastructure-based (i.e. non ad hoc), have mobile sensor nodes, etc. At that time the WSN research papers focused only on the theoretical and broad applicative uses of WSNs (e.g. military, environment, healthcare),

* Corresponding author. Tel.: +386 40 303 874.
E-mail addresses: muhamed.turkanovic@gmail.com (M. Turkanović), bostjan.brumen@um.si (B. Brumen), marko.holbl@um.si (M. Hölbl).

http://dx.doi.org/10.1016/j.adhoc.2014.03.009
1570-8705/

but the research and applicative use of WSN has significantly increased over the last few years. Today we talk about the use of WSN for traffic monitoring [3], pipeline monitoring [4], landslide detection [5], methane leak detection [6], border patrol [7], precision agriculture [8], rehabilitation applications [9], laboratory tutoring [10], asset tracking [11], real-time soccer playing monitoring [12] and many more [13–16]. A list of real-life applicative WSN projects was summed up by Romer and Mattern [2].

In the beginning it was thought that WSN would only be homogeneous, consisting only of equal sensor nodes. Today we also talk of heterogeneous WSNs since sensor networks can be built with different types of nodes, some more computationally-powerful than others (e.g. gateway nodes). In view of the IOT notion, the heterogeneity of a WSN is not the only thing rapidly adapting, hence the infrastructure has moved from mainly infrastructure-based networks, where nodes can only communicate directly with the base station, to ad hoc networks whereby nodes can also communicate directly with each other and with rest of the world.

WSNs are becoming evermore numerous and interconnected with the IOT, thereby presenting new opportunities but also challenges which need to be addressed. An example of such would be a remote user who wants to access a particular sensor node of the WSN. Such a user needs to be authorized and, if done positively, allowed to gather data from or send commands to the sensor node. Since the most important and distinct characteristic of WSNs is their resource-constrained architecture (i.e., limited computational and communicational capabilities), a lightweight security solution is required, thus urging the security design to be more prudent.

A key challenge is how to enable the establishment of a shared cryptographic key in a secure and lightweight manner, between the sensor node and the user outside the network. Mutual authentication is also needed for such a scenario, and is highly important since all parties need to be sure of the legitimacies of all the entities involved. Numerous cryptographic schemes for the security of the WSN have been proposed but very few have addressed the aforementioned scenarios, challenges, and requirements [17–27]. This was the motivation for us to develop and propose a challenge-specific cryptographic scheme, which uses a rare four-step authentication model that we believe is the most appropriate for the mentioned scenario, when a remote user wants to connect to a sensor node inside a WSN. Since our scheme uses smart cards for users to authenticate, the security architecture is also smart-card oriented. The proposed scheme is also lightweight and resource-friendly, hence it is based only on symmetric cryptography, whereby using only hash and XOR computation.

The remainder of the paper is organized as follows. Section 2 for better understanding of the topic below, provides some brief preliminaries. We present an overview of the existing work in Section 3. Our proposed mutual authentication and key agreement scheme for heterogeneous wireless sensor ad hoc networks is presented in Section 4, followed by the security and performance evaluations in Sections 5 and 6. Finally, Section 7 concludes the paper.

2. Preliminaries

Heterogeneous WSN consists of multiple, simple, low-cost sensor nodes that have limited computational and communicational capabilities and of at least one sink node, also called gateway node (GWN) [28]. GWN are bigger, more secure and have more computational and communicational capabilities. Since they are more powerful, they are being used to act as proxies between the sensor network and the outside world. Their functionalities are sometimes gathering and processing data from each sensor node before forwarding non-redundant information, sending commands to the sensor network, facilitating authentication schemes, etc. [29]. By facilitating with authenticated schemes, the GWN help to process mutual authentication and key agreement protocols by playing the lightweight role of a trusted third party entity [27].

According to Xue et al. [27] there are five basic authentication models for WSNs, and to our knowledge, this is the first time that authentication models for the WSN, based on the GWN, have been presented and depicted. Each of the five presented authentication models needs four messages to complete key agreement and mutual authentication. Since WSNs are resource constrained it is very important to reduce communication and transmission to the minimum, since the cost of transmitting 1 Kb of information is 3 J or equal to that of 80,000–600,000 instructions [30,31]. In four of the five models, the user initiates the key agreement scheme between him/her and the sensor node, by firstly contacting the GWN. The further key agreement communication depends on the specific model. The end result is always mutual authentication between all parties and a successful key agreement between the user and a specific sensor node.

When developing our novel mutual authentication and key agreement scheme for heterogeneous wireless sensor ad hoc networks, we focused on the resource constrained architecture of WSN, on the security requirements, and on the IOT-notional environment. According to our specifications and the mentioned requirements in the previous section for WSNs based on the IOT notion, we used the fifth authentication model (Fig. 1), described by Xue et al. [27]. This model is the only one which initiates the authentication and key agreement protocol by firstly contacting the specific sensor node. This approach has already been presented and used by Yeh et al. [23] in their secured authentication protocol for WSN using Elliptic Curve Cryptography (ECC). Using this authentication model, after successful registration, the remote user can reach a specific sensor node directly through the Internet and does not need to first connect with the GWN, thereby ensuring a more straightforward approach.

There are three types of cryptographic techniques for the WSN developed so far, i.e. symmetric, asymmetric, and hybrid [32]. Since WSNs are resource-constrained, the more lightweight techniques like the symmetric ones are the more appropriate. Even though symmetric based cryptographic schemes require less computational power, they need more memory for saving all the keys involved in the network (i.e. between all the nodes and users). Regardless to this, its efficiency still prevails in relation