Computer Networks 104 (2016) 137–154

Contents lists available at ScienceDirect

Computer Networks

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

Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines

Shipra Kumari*, Hari Om

Department of Computer Science and Engineering, Indian School of Mines, Dhanbad, India

ARTICLE INFO

Article history:
Received 8 December 2015
Revised 6 May 2016
Accepted 11 May 2016
Available online 12 May 2016

Keywords:
Mechanical sensor
Authentication
Hash function
Session Key agreement

ABSTRACT

The goal of this paper is to find the requirement and security issues of wireless sensor networks (WSNs) especially in coal mines for safety monitoring and to develop an authentication protocol to provide the security in WSNs. The WSNs help in reducing the hazard and increase the productivity by proper monitoring the equipments and underground conditions. In mines, a sensor in a WSN senses the environment and transmits the data to colliery professionals for further detailed assessment as a minor factual error may cause severe human casualties and large resource destruction that may lead to huge monetary losses. The sensors have limited battery that should be used efficiently in computing the acquired information. In this paper, we present an authentication protocol to overcome the security issues in WSNs by authenticating the users (professionals) and the mechanical sensors. Our protocol requires only light weight functions and low cost in transmission of the messages to save the battery in sensors. We use the BAN (Burrows-Abadi-Needham) logic to ensure the mutual authentication and session key agreement properties. The formal security analysis proves its resilience against various security attacks. For its formal security verification, a widely accepted AVIPSA (Automated Validation of Internet Security Protocols and Applications) tool is used.

1. Introduction

A WSN consists of tiny, autonomous, and compact devices, called sensor nodes, that are deployed in remote areas to detect/monitor an event, collect data and process it, and then transmit it to users [4]. A sensor node in a WSN is of small size that is capable of sensing, gathering, and processing the data while communicating with other nodes via a radio frequency (RF) channel. The multifunctional sensors with low-cost and low-power consumption have received increasingly attention from various industries. The sensor networks have been discussed for various applications due to their ability for monitoring and detecting possible hazardous events in critical areas such as underground mines, vacano, flood, etc. Due to technological advancements in sensors, microelectronics, networks, and wireless communication, the WSNs are being applied widely in military, medical, building condition monitoring, wildlife monitoring, environmental monitoring, etc. In some emergent situations, the wireless communication may become vital for survival, for instance, during a disaster such as fire, rock falls, where the conventional wired communication systems may not be feasible. Environment monitoring in underground tunnels, which are usually long and narrow, ranging in length of tens of kilometers and widths of meters, has been a crucial task to ensure safe working conditions in coal mines. The safety problems of coal mines have gradually become the nation and society concerns. Most of the process control applications are exceptionally crucial jobs and have rigorous requirements. Therefore, a continuous monitoring of underground environment is needed to reduce these disasters.

The coal is one of the primary energy sources in India that provides over 54.5% of the total energy [1]. Coal mining is, however, one of the world's most dangerous occupations. As the underground mining becomes deeper and deeper and the earth stress increases, the influence of rock movement caused by mining makes mine safety situation further severe. The mine accidents have been a frequent phenomenon in coal belt [2,35,36,41]. There were 74 miners casualties in Gaslitand, Dhanbad, on September 26, 1995 and 55 in the New Kenda Colliery in 1994. There were 375 workers who lost their lives in the Chasnala coal mine disaster in December 1975. Since the dynamite is used for coal-mining operations, sometimes the explosion leaves a big crack and the water from a nearby tank or river floods the mine. Both in the Chasnala and Gaslitand disasters, the water from a nearby reservoir and a rain-fed river rushed into the mines that broke the barrier walls

* Corresponding author.
E-mail addresses: shiprakumari18jan@gmail.com (S. Kumari), hariom4india@gmail.com (H. Om).

http://dx.doi.org/10.1016/j.comnet.2016.05.007
1389-1286/© 2016 Elsevier B.V. All rights reserved.

and the workers were trapped in the flooded mines. In 1965, there was an explosion at Dhori colliery near Dhanbad that led to a fire in the mines, resulting in the loss of 268 lives. There have been a huge number of deaths in different countries in mine accidents, but to meet ever-higher production targets, the mine safety measures have not received adequate attention. The miners and other persons involved in mining face many dangers on the job. Some of the important reasons for occurring the above mentioned type hazards are due to the following [42]:

- When the walls and ceilings of the underground mine shafts have not been properly secured.
- If a mine shaft is excavated too deeply that may lead to cracks in the floor and walls of the shaft, weakening the structure.
- Improperly planned drill and blasting activities can cause cave-ins if exclusion zones are not correctly mapped.
- Gas explosions often occur in coal mines from a build-up of methane gas due to lack of ventilation.
- Explosions can easily be triggered by a spark in cables or plugs used in heavy electrical equipments.
- Collisions of large equipments or crushing.
- Water leveling of the roadway not accurately measured.
- If the mining environment is damp, the workers can easily be electrocuted due to heavy electrical devices.
- A fire can occur in mines for a range of reasons, the most common being gas leaks, electrical faults, and the spillage of flammable chemicals.

Using WSNs, the professionals can detect the exact fire location and its spreading direction to provide the fire prevention system that can resist the loss of natural resources and human causalities. Gas levels can also be monitored frequently to prohibit the major accidents in coal mines by checking the level of legislated amount and evacuating the areas if the level exceeds. The CO-sensor, smoke sensor, temperature sensor, low frequency acoustic sensor, pump status, sensor water level sensor, etc. are some types of sensors being used in coal mines [3]. The sensors can also provide the information about the width of a wall so that the authorities can give the command to stop blasting and save the wall or floor from the crack. The WSNs reduce the investment on underground lines-laying and maintenance difficulties, ensure timely, accurate, and rapid transmission of data in all key underground mining zones and improve the system efficiency [5–10]. Moreover, to survive in a competitive market, the coal mines must use condition monitoring sensors to yield cost effective production. Cost effectiveness in mines depends on the maintenance cost of resources and machineries. The WSNs are used to monitor the remote machines online from a central location. The technicians can then be deployed at those remote locations only where the maintenance is actually needed to save the operating and maintenance costs. Though adopting the WSN technology to process control systems is attractive, yet there are several challenges [18,19,21]. The transition from wire to wireless can be beneficial only if the related issues are resolved by the combined efforts from both academia and industry. The WSNs have attracted researchers across interdisciplinary areas such as management, electronics and computer, industries, software engineering, etc. Some computer-controlled coal mine safety monitoring systems have been discussed in [11–17]. Process monitoring and control applications range from data sensing, measurement, record, and diagnosis, to machinery/equipment operation and emergency action. For smooth operation, the major concern is the quality of service that requires the correct data at the right time, i.e., the reliability of data and the real-time guarantee. Due to several attacks, secure transmission is one of the major concerns for WSN applications to obtain reliable data. The attacks vary from eavesdropping on transmissions, including traffic analysis or disclosure of message contents to modification, fabrication, and interruption of transmissions through node capturing, routing attacks [20]. As a result, the internal facts about the machinery conditions and mines could expose to illegal users (e.g., insurance agents, media persons, business competitors, etc.), which may lead to further complications. The modified or fabricated data can misguide the professionals and they may give incorrect commands which may lead to severe problems. Therefore, while designing a protocol all the security primitives should be addressed.

In this paper, we focus on the problem of authenticity to avoid unauthorized access to the information in WSNs in general and in coal mines in particular to resist an attacker to get into the system and harm it. The user authentication in WSNs is a critical security concern to assure the secure communication. For example, suppose a colliery professional wants to communicate with a sensor that senses the wall width in underground mines to stop further coal blasting. In mines, it is necessary to maintain the minimum width of the wall to avoid leakage of water from the other side of the wall. For this purpose, the system first tries to authenticate the professional and the sensor to ensure their legitimacy before actual data transmission. If a system fails to securely authenticate the legal communicating parties and an attacker finds a way in the communication between them, then he may fabricate wrong information such as incorrect wall width measurement and send it to the professional. In this case, the legal professional may give a misguided command to more blasting of the coal wall, even if the minimum limit has already reached. A major hazard may occur due to such lack in safety monitoring. Thus, this type of lack in safety monitoring occurs due to improper verification of the communicating parties who share highly sensitive information. Additionally, the protocol must be cost-effective in terms of computation and communication overheads, mainly for the sensor nodes. After discussing the necessity of WSNs particularly in coal mines and the authentication problem related to it, we propose an efficient authentication protocol to prove the legitimacy of all the participating parties (namely, user, gateway, and sensor) for proper safety monitoring.

The rest of the paper is organized as follows. Section 2 reviews the literature to discuss the pros and cons of the existing authentication protocols for WSNs. In Section 3, we present the attacker model that describes the capabilities of an adversary to get into the system. In this section, we also present the notations used in our proposed protocol and properties of the one-way hash function. Section 4 presents the proposed authentication and key agreement protocol in WSNs to authenticate the colliary professionals and the sensors. Section 5 provides the detailed security analysis of the proposed protocol to justify the claim that it is very safe against all the known attacks. Section 6 provides the proof of authentication and key agreement in our protocol using BAN logic. In Section 7, we simulate and formally analyze our protocol using the AVISPA tool. Section 8 presents the performance evaluation of our protocol to prove its fruitfulness over the existing protocols. Finally, in Section 9, we draw our conclusion and also the future work.

2. Literature review

The main challenge in WSNs is to provide strong security with low overhead to a sensor. In last few years, various authentication protocols [22–30] have been developed to provide security in a WSN environment. In a WSN, a remote authorized user is allowed to access a reliable sensor. Since the sensor nodes are equipped with the limited computing power, storage, and communication modules, it is important to design a secure, effective, and lightweight, authentication and key agreement protocol. The authentication protocols for WSNs have become a popular choice for the researchers due to their large applications.