Computer Networks 105 (2016) 60–74

Contents lists available at ScienceDirect

Computer Networks

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

Review article

A survey of key management schemes in multi-phase wireless sensor networks

Mohamed-Lamine Messai[a,*], Hamida Seba[b]

[a] *Département d'informatique, Faculté de sciences, Université de Sétif 1, 19000 Sétif, Algérie*
[b] *Université de Lyon, CNRS, Université Lyon 1, LIRIS, UMR5205, F-69622, France*

ARTICLE INFO

Article history:
Received 8 April 2015
Revised 17 April 2016
Accepted 10 May 2016
Available online 24 May 2016

Keywords:
Key pre-distribution
Key management
Multi-phase wireless sensor networks
Generation keys
Self-healing

ABSTRACT

Wireless Sensor Networks (WSNs) are the enabling technology for smart cities, intelligent cars and transportation systems, precision agriculture, animal tracking, and all data collection and sensing-based applications. In most WSN applications, new sensor nodes are added to the network by post-deployment to assure network connectivity, to replace dead sensor nodes or to cover more regions in the area of interest. This type of network is called *Multi-Phase* WSNs (MPWSNs). Similarly to classical WSNs, *multi-phase* WSNs require security mechanisms to ensure their deployment. However, these networks need specific solutions adapted to the multiple deployments of nodes. In this paper, we review, classify and compare the existing key management schemes proposed for this type of sensor network. We illustrate both advantages and disadvantages of each multi-phase key management scheme. Finally, we give some directions to design lightweight robust key management for MPWSNs.

1. *Multi-phase* WSNs, principle and applications

Nowadays, Wireless Sensor Networks (WSNs) are a confirmed technology designed to sense and collect data in various domains and mainly those where human access is difficult, dangerous or unfeasible: forest fire detection, natural phenomena surveillance (i.e., volcano, hurricane, etc.), battlefield supervision, etc. In these kinds of applications, sensor nodes are intended to work in total autonomy. They are powered through non-rechargeable batteries and collaborate to deliver the collected data hop by hop to some processing center (called generally sink node or base station) [1,2]. Hop by hop transmission is motivated by two main reasons:

1. It uses a short transmission range which remedies the energy constraint related to batteries of these miniature sensing devices [3].
2. It allows a possible aggregation of redundant data at intermediate nodes. This aggregation will reduce significantly the number of forwarded packets to the sink [4].

However, hop by hop communications require network connectivity which can depend on the environmental conditions (flat area, mountainous region, field with obstacles, etc.) where sensor nodes are deployed. Connectivity may be affected when sensor nodes with low energy could not reach long distances. In fact, the sensor nodes of a network do not all die at the same time. Routing, security, and aggregation protocols assign different tasks to nodes. This is the main reason why some nodes die faster than others. Therefore, in most cases, new sensor nodes are added by a post-deployment to an existing WSN. This type of network is called *Multi-Phase* WSNs (MPWSNs). A MPWSN is defined as a network where new groups of sensor nodes are added in the area of interest at fixed periods or at random times named phases. Each group of nodes deployed together at the same phase is called a generation. The lifetime of a MPWSN is expanded as long as there are new generations that join the network. Multi-phase deployment of nodes offers the following benefits:

1. It is a manner to provide a maximum lifetime to a WSN.
2. It ensures the expandability of applications (e.g. to cover more regions in the area of interest).
3. It guarantees network connectivity by replacing the dead sensor nodes in critical positions such as those situated close to the base station. This will avoid network disconnection.
4. It enhances network security especially where it is exposed to node capture attacks.

Fig. 1 displays an example of a post-deployment where newly deployed nodes provide continuity to network connectivity. The bold nodes are newly deployed and are mandatory to ensure

[*] Corresponding author.
E-mail address: messai.amine@gmail.com, messai.amine@univ-setif.dz (M.-L. Messai).

http://dx.doi.org/10.1016/j.comnet.2016.05.005
1389-1286/

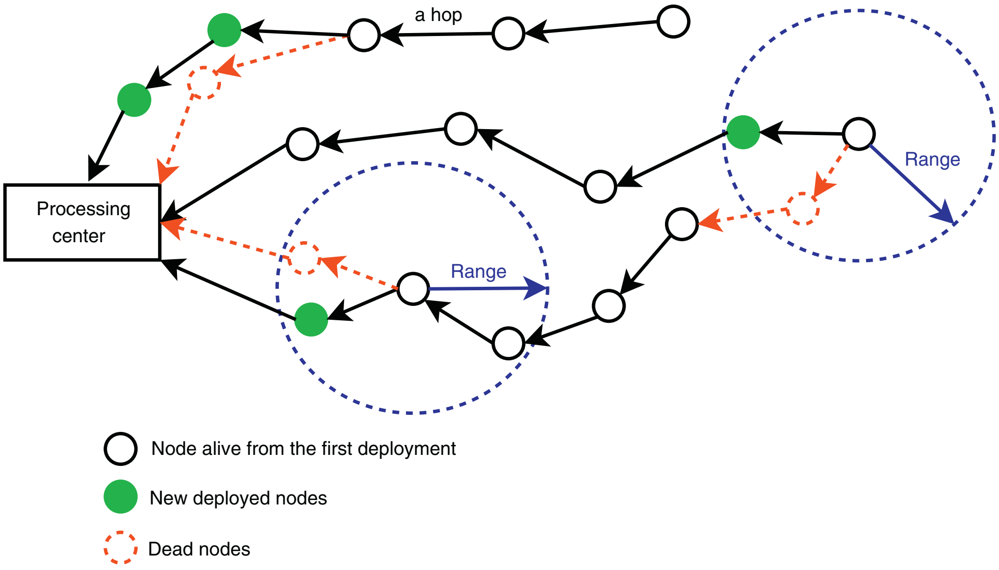

Fig. 1. An example of a post-deployment.

network connectivity. They replace the dead nodes represented with dashed lines.

To achieve the benefits of multi-phase deployment, some obstacles must be overcome and, in particular, the security aspect, which is the most important issue with respect to hostile places where the sensor nodes may be deployed. In view of the post-deployment particularity in MPWSNs, secure communications, assuring confidentiality, authentication and data integrity, should be established between nodes deployed at different times. For example, the message exchange between nodes (that are still alive) of the first deployment and other nodes issued from different post-deployments must be secured.

Key management is an essential element for providing security in any network. It consists It consists in computing or distributing a common secret that will serve to ensure confidentiality and integrity of communications between sensor nodes. This task is not easy to achieve in WSNs because:

1. For cheapness and dense deployment purposes, sensor nodes cannot be tamper-resistant devices.
2. Sensor nodes are scattered alone in unattended environments and should operate in hostile conditions in some applications. An adversary can easily capture a sensor node by physically accessing and then compromising its security material (keys, cryptographic algorithm, etc.).

Many key management approaches are proposed for WSNs. However, these approaches are designed to solve the key management problem mainly in single phase WSNs, and their security in MPWSNs degrades with time when adversaries compromise nodes.

So, new key management schemes are proposed to allow nodes of different generations to establish pairwise keys and to offer the resistance against node compromising attacks [5–17]. The proposed schemes employ a key refresh at each generation to limit the effectiveness of adversaries. Consequently, compromised keys are harmful only for a short period of time. For the key refresh operation, a basic idea would be to pre-distribute the nodes of each generation with random independent keys. When we use new randomly generated keys at each generation, adversaries cannot guess the upcoming keys by knowing previous or current ones. However, with this solution, the sensor nodes deployed at different generations may not establish secure communications (no shared keys). So, in order to achieve key connectivity between nodes belonging to different generations, the following two methods are used:

- The keys to use in the next generation are derived from keys of the current generation (generally by using a hash function). So, there is some kind of relation between the keys of different generations.
- Each sensor node of the current generation is pre-distributed with a set of keys that will be used in some next generations.

Several papers survey key management schemes in WSNs [18–24]. However, to the best of our knowledge, no review paper considers key management schemes in WSNs where nodes are deployed in generations.

The succession of sections in this paper is organized as follows. First, the next section lists the contributions and explains the novelty of our paper compared to existing ones. In Section 3, we describe the adversary model and define the evaluation metrics that should be considered when designing key management for MPWSNs. Section 4 overviews the existing proposed key management schemes in MPWSNs. According to the given evaluation metrics, Section 5 presents a comparison of the studied schemes. Finally, we conclude by giving some research directions in Section 6.

2. Contribution

Key management schemes in WSNs are surveyed in several papers [18–29]. Zhang et al. in [18] classify key management schemes in WSNs in three classes based on the encryption techniques: symmetric, asymmetric and hybrid. They describe and discuss key management solutions within these three classes. Xiaobing et al. [19] describe dynamic key management schemes in WSNs. They classify them in two categories: distributed and centralized. A key management scheme is dynamic when the pairwise keys are refreshed periodically or on demand. In [20], Xiangqian et al. studied the vulnerabilities and security issues in WSNs. They summarize the advantages and disadvantages of some key management schemes in WSNs. In [21], the authors present the different key management schemes in WSNs with eight classes: network-wide key schemes, full-pairwise schemes, probabilistic schemes, matrix-based schemes, polynomial-based schemes, combinatorial design schemes, and deployment knowledge based schemes. In the class of probabilistic schemes, the authors address multiple deployments