Journal of Network and Computer Applications 34 (2011) 1302–1325

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

Anomaly detection in wireless sensor networks: A survey

Miao Xie *,[1], Song Han *, Biming Tian, Sazia Parvin

Digital Ecosystems and Business Intelligence Institute, Curtin University, DEBII, GPO Box U1987, Perth, WA 6845, Australia

ARTICLE INFO

Article history:
Received 19 August 2010
Received in revised form
10 February 2011
Accepted 7 March 2011
Available online 21 March 2011

Keywords:
Wireless sensor networks
Information security
Anomaly detection

ABSTRACT

Since security threats to WSNs are increasingly being diversified and deliberate, prevention-based techniques alone can no longer provide WSNs with adequate security. However, detection-based techniques might be effective in collaboration with prevention-based techniques for securing WSNs. As a significant branch of detection-based techniques, the research of anomaly detection in wired networks and wireless ad hoc networks is already quite mature, but such solutions can be rarely applied to WSNs without any change, because WSNs are characterized by constrained resources, such as limited energy, weak computation capability, poor memory, short communication range, etc. The development of anomaly detection techniques suitable for WSNs is therefore regarded as an essential research area, which will enable WSNs to be much more secure and reliable. In this survey paper, a few of the key design principles relating to the development of anomaly detection techniques in WSNs are discussed in particular. Then, the state-of-the-art techniques of anomaly detection in WSNs are systematically introduced, according to WSNs' architectures (Hierarchical/Flat) and detection technique categories (statistical techniques, rule based, data mining, computational intelligence, game theory, graph based, and hybrid, etc.). The analyses and comparisons of the approaches that belong to a similar technique category are represented technically, followed by a brief discussion towards the potential research areas in the near future and conclusion.

1. Introduction

A wireless sensor network (WSN) is made up of a mass of spatially distributed autonomous sensors, to jointly monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion and pollutants (Yick et al., 2008). To date, WSNs have been successfully applied to many industrial and civil domains, including industrial process, monitoring and control, machine health monitoring, environment and habitat monitoring, healthcare applications, home automation, and traffic control. A typical WSN has little or no infrastructure. If the deployment of a WSN is subject to an ad hoc manner, it is categorized as unstructured. In contrast, the network deployed with a pre-planned manner is categorized as structured. Each sensor node is optionally built up with a variety of network services such as localization, coverage, synchronization, data compression and aggregation, and security, for the purpose of enhancing the network's overall performance. Sensor nodes communicate with each other, through following the typical five-layer communication protocol stack, which consists of physical layer, data link layer, network layer, transport layer, and application layer.

The properties of WSN inevitably cause that a sensor node is extremely restricted by resources, including energy, memory, computing, bandwidth, and communication. Hence, WSN is vulnerable to security threats both external and internal. In addition, physical access is allowed for sensor nodes, as the network is usually deployed near the physical source of the event, but without tamper-resistance owing to cost constraint. What is worse, the information exchange can be captured by any internal and external devices, caused by the use of publicly accessible communication channels. In consequence, a WSN is often threatened by multiple security threats, which could be categorized as follows (Lopez and Zhou, 2008):

- communication attack;
- denial of service attack;
- node compromise;
- impersonation attack;
- protocol-specific attack.

Han et al. (2005) also propose a good taxonomy that surveys the security threats according to a more detailed criteria.

Securing WSN is imperative and challenging accordingly. Prevention-based techniques that fundamentally build upon

* Corresponding authors.
E-mail addresses: clifford1984621@gmail.com (M. Xie), hansongau@gmail.com (S. Han).
[1] Tel.: +61 040 1400624.

1084-8045/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2011.03.004

cryptography are the first line of defense for protecting WSN. Based on a primitive of secret key management, encryption and authentication are the primary measures in a prevention-based technique, as that introduced in the security framework SPINS (Perrig et al., 2001). However, in case the first line of defense is broken through, compromised nodes could extract security-sensitive information (e.g. secret key), leading to breaches of security. Thus, developing detection-based techniques as the second line of defense appears to be of great importance. Intrusion detection is a typical example of detection-based techniques. This concept was originally proposed by Anderson (1980) two decades ago in a report "Computer Security Threat Monitoring and Surveillance". Intrusion detection is defined as the process of monitoring the events occurring in a computer system or network and analyzing them for any signs of possible incidents, which are violations or imminent threats of violation of computer policies, acceptable use policies, or standard practices (Scarfone and Mell, 2007). However, anomaly detection (Hu, 2010, also referred as outlier detection, deviation detection, etc.), a branch of intrusion detection, is best suited to WSN because its methodology is flexible and resource-friendly in general. Anomaly detection is defined as the process of comparing definitions of activity that is considered normal against observed events in order to identify significant deviations. Moreover, an anomaly in a dataset is defined as an observation that appears to be inconsistent with the remainder of the dataset (Hodge and Justin, 2004).

Anomaly may be caused by not only security threats, but also faulty sensor nodes in the network or unusual phenomena in the monitoring zone (Rajasegarar et al., 2008). In the real world, isolated node failures can bring down the entire network, which is harmful to reliability of WSN. This survey paper merely focuses on anomaly detection techniques in WSN, irrespective of causes of generating anomaly. The overview of the content of this survey paper is given in Fig. 1.

1.1. Motivation

The research relating to anomaly detection in WSN has been followed with much interest in recent years. From the ISSNIP (Intelligent Sensors, Sensor Networks and Information Processing, The University of Melbourne, Australia) group, Rajasegarar et al. (2008) did a survey on the related works before 2007 with a simpler criteria: statistical parameter estimation techniques or non-parametric techniques. Nevertheless, a technology-concerned survey is yet absent to present the latest progress of developing anomaly detection in WSN.

Moreover, our paper expects acting as a guideline of selecting appropriate anomaly detection techniques. Through analyzing and comparing those particular approaches that belong to a similar technique category, the advantages and shortcomings of each technique category can be identified. Accordingly, it further extracts the key design principles to overcome possible flaws.

The pattern of anomaly detection significantly impacts on the performance of a detection scheme, which basically relates to who is mainly responsible for the data processing of detection. The choice of detection pattern depends on the application scenario. The fair understanding with regard to these available anomaly detection patterns could facilitate the development of detection schemes. In consequence, these anomaly detection patterns are surveyed separately in this paper.

In our survey paper, all detection schemes are divided into two types of detection method: prior-knowledge based, or prior-knowledge free. The prior-knowledge-based detection schemes are better suited to the applications which are biased to detection speed; the prior-knowledge free schemes, on the contrary, are capable of providing applications with stronger detection generality. This awareness is positive to optimally selecting anomaly detection techniques. Attribute selection is traditionally a critical issue in a detection system, as using less number of attributes is able to conserve resource. Our paper emphasizes the importance of this issue for developing anomaly detectors in WSNs, whereas a detailed discussion is not given owing to space constraint.

Finally, the developing orientations in this area are examined, and a number of potential research areas in the near future are proposed.

1.2. State-of-the-art techniques

Other than anomaly detection, there are also misuse/signature detection and stateful protocol analysis in the category of intrusion detection (Scarfone and Mell, 2007). Misuse/signature detection is defined as a process of comparing signatures against observed events to identify possible incidents, where each signature is a pattern corresponding to a known threat. Stateful protocol analysis is defined as the process of comparing predetermined profiles of generally accepted definitions of benign

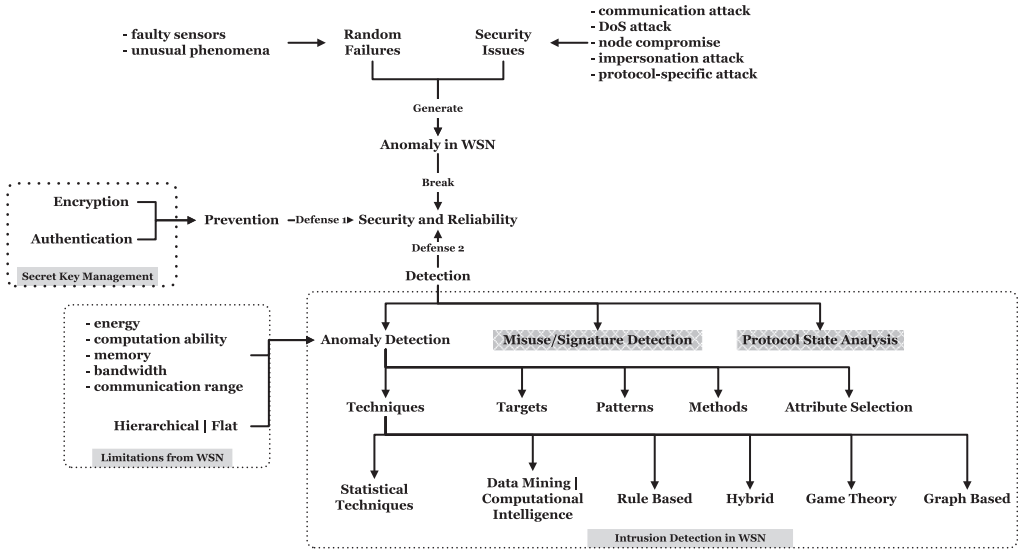

Fig. 1. The content of this survey paper.