Analyses of Intrusion Detection Model in Wireless Sensor Networks

김정태
목원대학교

무선 센서 네트워크에서의 침입탐지 모델의 분석

Jung-Tae Kim
Mokwon University
E-mail : jtkim5068@gmail.com

요 약

Intrusion detection in Wireless Sensor Network (WSN) is of practical interest in many applications such as detecting an intruder in a battlefield. The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. For this purpose, it is a fundamental issue to characterize the WSN parameters such as node density and sensing range in terms of a desirable detection probability. In this paper, we consider this issue according to two WSN models: homogeneous and heterogeneous WSN.

Ⅰ. Introduction

As wireless sensor networks are becoming prevalent and widely used in mission critical systems and environments, their security is becoming a never-growing concern. Wireless sensor networks (WSNs) are vulnerable to various attacks since they are distributed in unattended environments and have limited energy, storage and computation abilities. Preventive approaches can be applied to protect WSNs from some kinds of attacks.

Due to their deployments in remote and frequently hostile environments, combined with device constraints, WSNs are particularly vulnerable to attacks from adversaries. Some security protocols or mechanisms have been designed for sensor networks. For example, SPINS (Sensor Protocol for Information via Negotiation), a set of protocols, provides secure data confidentiality, two-party data authentication, and data freshness and authenticated broadcast for sensor network [1]. LEAP (Localized Encryption and Authentication Protocol), is designed to support in-network processing bases on the different security requirements for different types of messages exchange [2]. Several schemes have been proposed to detect intrusions in wireless sensor networks. However, most of them aim on some specific attacks or attacks on particular layers, such as routing layer or media access layer.

II. Related Work

Recently, a number of research efforts have been made to develop sensor hardware and network architectures in order to effectively deploy WSNs for a variety of applications. Due to a wide diversity of WSN application

requirements, however, a general-purpose WSN design cannot fulfill the needs of all applications. Many network parameters such as sensing range, transmission range, and node density have to be carefully considered at the network design stage, according to specific applications. There are two detection models in terms of how many sensors are required to recognize an intruder: single-sensing detection model and multiple-sensing detection model. It is said that the intruder is detected under the single-sensing detection model if the intruder can be identified by using the sensing knowledge from one single sensor. On the contrary, in the multiple-sensing detection model, the intruder can only be identified by using cooperative knowledge from at least k sensors IDS framework normally consists of misuse detection and anomaly detection. In [3], Doumit and Agrawal have proposed an anomaly approach, namely, "Self-Organized Criticality & Stochastic Learning Based IDS", based on the structure of naturally occurring events.

A. Agah et al. [4] have proposed Anon-cooperative Game Approach, "a game theoretic framework for defending nodes in a sensor network". Piya Techateerawat et al.[5] have investigated three static strategies in a set of nodes, including "core defense", "boundary defense" and "distributed defense". In this paper, we also make a comparison of energy efficiency of the three strategies.

III. Concept of IDS

The network structure of intrusion detection system is shown in figure 1. For assuring full network coverage, a decentralized architecture must be used, because any part of the network can be a possible point of intrusion. As a result, the detection tasks must be performed by a software element (i.e., agent) located inside every node (node agents), and in every base station (base station agents). These

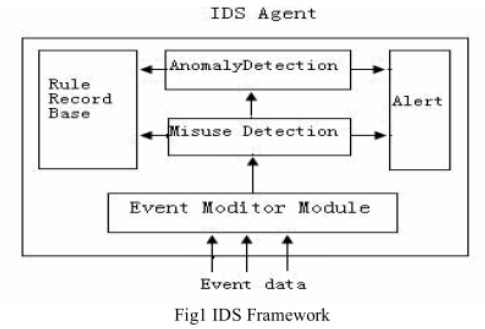

Fig1 IDS Framework

Figure 1. Configuration of IDS framework

two types of agents have different capabilities and use different sources of information. A sensor node is very constrained by nature, thus its node agent should employ only lightweight mechanisms. Also, the node agent can obtain information only from its direct neighborhood. On the other hand, the powerful base station receives information from all the nodes in the network, thus the base station agent can take advantage of this wealth of information to observe and analyze the behavior of its nodes. Wireless local area network builds with wireless mesh network. Every nodes of wireless mesh network is a router as well as an access point. Node can send and receive information and directly communicate with one or more equity nodes, convenient fix, non-line-of-sight transmission, better robustness, flexible structure, high-bandwidth etc. In order to evaluate the quality of intrusion detection in WSNs, we define three metrics as follows:

. Intrusion distance.

The intrusion distance, denoted by D, is the distance that the intruder travels before it is detected by a WSN for the first time. Specifically, it is the distance

between the point, where the intruder enters the WSN and the point where the intruder gets detected by any sensor(s). Following the definition of intrusion distance, the Maximal Intrusion Distance (denoted by ר, ר > 0) is the maximal distance allowable for the intruder to move before it is detected by the WSN.

. Detection probability.

The detection probability is defined as the probability that an intruder is detected within a certain intrusion distance.

. Average intrusion distance.

The average intrusion distance is defined as the expected distance that the intruder travels before it is detected by the WSN for the first time [6]. After deploying sensor nodes, we format clusters according clustering formation algorithm. Secondly, activate IDS in certain nodes in clusters to detect intruders. Due to different energy overheads in nodes, new cluster will differ from the original one according to clustering reconfiguration algorithm every time. Take cluster heads for example, cluster heads will change every time after reconfiguration. So the clusters are changing at intervals and IDS are moving as well, which forms a dynamic model. Dynamic IDS Algorithm in detail as follows: [7].

Step 1: Cluster Formation

On the issue of cluster formation, a lot of researches have been done. Here, we choose an algorithm, "Energy-Efficient Cluster Formation for Large Sensor Networks using a Minimum Separation Distance", which is developed from a classic algorithm LEACH.

Step 2: Activate IDS

Activate IDS pre-installed in cluster heads and boundary nodes. Let them take the detection task. In other words, we adopt core defense and boundary defense together in a cluster.

Step 3: Cluster Reconfiguration

If any IDS node in clusters has consumed 30 percent of energy which it has before running IDS, launch clusters reconfiguration process. Here we choose a cluster reconfiguration algorithm called 'Energy-Efficient Clustering System Model and Reconfiguration Schemes for Wireless Sensor Networks'.

Step 4: Activate IDS in new Clusters

After cluster reconfiguration, activate IDS in cluster heads and boundary nodes in new clusters. Let them taken the detection task.

Step 5: Upgrade Defense Structure

When number of intruders which has been detected in unit time in a cluster is bigger than a defined threshold, the algorithm will upgrade core defense and boundary defense to distribute defense which has stronger detection capability.

Step 6: return to step 3, repeating.

IV. Elements of IDS

We first consider attack models as follows. The attack models can be summarized as follows:

A. Route Loop
B. Jamming Attack
C. Sinkhole Attack
D. Wormhole Attack
E. Blackhole Attack

Before discussing the IDS model, we make the follow-ing assumptions:

1) The nodes are stationary and no new nodes are added into the network.
2) Data packets flow to the sink node and the network uses tree based forwarding mechanism for routing.
3) Tampered nodes perform normally except for making an attack.
4) There is enough training time before attacks start.

To implement an effective IDS for wireless networks as outlined in [8], the

system needs to be able to guard against certain security vulnerabilities that make a wireless network much more prone to attacks than traditional wired networks. Some of these additional security measures include the following:

1. Each node must be able to utilize only the traffic coming in and out of the node as audit data.
2. Each node must be capable of detecting and potentially handling attacks from within the network as well as external to the network.
3. Each node must be able to determine the presence of an attack despite having a limited amount of communication with other nodes.
4. Each node has to accomplish these necessary tasks using limited power and processing resources. Particularly for defending against DoS attacks, the article indicates that a key step towards identifying malicious nodes is to determine if a node is generating a greater number of packets than a specified threshold during a designated time interval. While designing and implementing our system to be an "effective and efficient IDS", we have taken some of these key points into consideration.

VI. Conclusion

In this paper, we focused on IDS in WSN and proposed our dynamic IDS model (DIDS) for WSN comparing to static models (SIDS). We also analyzed performances of our dynamic model on security, stability and robustness issues. We found that our dynamic model had improved the three issues above better than static ones.

References

[1] A. Perrig, et al., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, 8(5):521- 534, Sep. 2002.

[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-scale Distributed Sensor Networks", Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03), Oct. 2003.

[3] Piya Techateerawat, Andrew Jennings."Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks", IEEE2006 WIC,2006

[4] S. Doumit and D.P. Agrawal,"Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor network", MILCOM 2003 - IEEE Military Communications Conference, vol. 22, no. 1, pp. 609-614, 2003

[5] A. Agah, S. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non-cooperative game approach", in 3rd IEEE International Symposium on Network Computing and Applications, (NCA2004), Boston, MA, August 2004, pp. 343346.

[6] Yun Wang, "Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 7, NO. 6, JUNE 2008, pp.698-711

[7] Guangcheng Huo , Xiaodong Wang, "A Dynamic Model of Intrusion Detection System in Wireless Sensor Networks ", Proceedings of the 2008 IEEE International Conference on Information and Automation June 20 -23, 2008, Zhangjiajie, China, pp.374-378

[8] A. Mishra, K. Nadkarni, A. Patcha, "Intrusion detection in wireless ad hoc networks" IEEE Wireless Communications, vol. 11 (1) (Feb. 2004):
pp. 48-60.