A Hybrid Intrusion Detection System for IoT Applications with Constrained Resources

Chao Wu, Chongqing Vehicle Test & Research Institute Co. Ltd., Chongqing, China

Yuan'an Liu, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China

Fan Wu, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China

Feng Liu, SKLOIS, IIE & SCS UCAS, CAS, Beijing, China

Hui Lu, Institute of Microelectronics of the Chinese Academy of Sciences, Beijing, China

Wenhao Fan, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China

Bihua Tang, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, China

ABSTRACT

Network security and network forensics technologies for the Internet of Things (IoT) need special consideration due to resource-constraints. Cybercrimes conducted in IoT focus on network information and energy sources. Graph theory is adopted to analyze the IoT network and a hybrid Intrusion Detection System (IDS) is proposed. The hybrid IDS consists of Centralized and Active Malicious Node Detection (CAMD) and Distributed and Passive EEA (Energy Exhaustion Attack) Resistance (DPER). CAMD is integrated in the genetic algorithm-based data gathering scheme. CAMD detects malicious nodes manipulated by cyber criminals and provides digital evidence for forensics. DPER is implemented in a set of communication protocols to alleviate the impact of EEA attacks. Simulation experiments conducted on NS-3 platform showed the hybrid IDS proposed detected and traced malicious nodes precisely without compromising energy efficiency. Besides, the impact of EEA attacks conducted by cyber criminals was effectively alleviated.

KEYWORDS

Cybercrime, Energy Efficiency, Genetic Algorithm, Graph Theory, Internet Of Things, Network Forensics

INTRODUCTION

Network forensics is the reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices (Schwartz, 2010). Network forensics technologies focus on recording evidence of a network attack (Adeyemi, Razak, & Nor Azhan, 2013). However, Internet of Things (IoT) is a special network which integrates sensors and other objects to connect everything in our life together. The information in IoT is usually privacy-sensitive and even confidential, so IoT will become the objective of cyber criminals (Alaba, Othman, Hashem, & Alotaibi, 2017). Due to the device miniaturization and energy-efficiency of IoT, traditional network forensics technologies are not suitable for IoT. Thus, the network forensics technologies specialized for cybercrimes aiming at IoT are of great importance and challenging in the era of IoT. Different from traditional computer networks, IoT networks are typically Low-power and Lossy Networks (LLN) (Teklemariam, Van Den Abeele, & et al, 2016), so energy efficiency must be taken into consideration when it comes to network security and network forensics technology designs for IoT.

DOI: 10.4018/IJDCF.2020010106

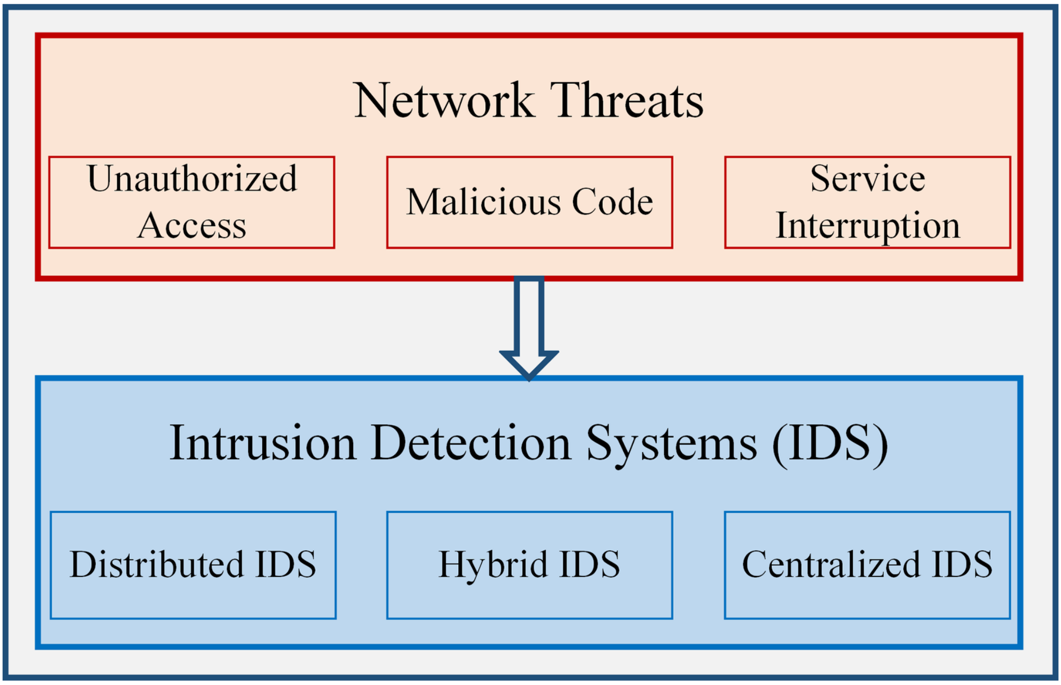
Intrusion Detection Systems (IDSs) can be categorized into three types by placement (Zarpelao, Miani, Kawakani, & de Alvarenga, 2017), as shown in Figure 1. Distributed IDS mean the detection system is placed in every physical node. Distributed IDSs are suitable for smart devices with higher computational capability and energy sources. Correspondingly, centralized IDS only rely on single or several dedicated components in the network to complete the detection work. Hybrid IDS combines distributed and centralized technologies to get the job done.

Aiming at computer networks, threats can be categorized into unauthorized access, malicious code and service interruption (Ahmed, 2017) as showed in Figure 1. In IoT networks, cyber criminals may manipulate data nodes in the network illegally, and generate plenty of fake or harmful information. Besides, unauthorized cyber criminals may access data nodes in IoT networks to perform Denial of Service (DoS) attacks. One form of DoS attacks in IoT is Energy Exhaustion Attack (EEA) (Alrajeh, Khan, Lloret, & Loo, 2014). EEA accelerates the expiration of the network lifetime and is fatal to the performance of IoT.

Sink mobility is recognized as an efficient method to improve the performance of IoT. However, mobility-constrained mobile sinks exist in many IoT applications, such as railway-based (Smeets, Shih, Zuniga, Hagemeier, & Marrón, 2013) or automobile-based (Huang & Savkin, 2016) information collection applications, mountainous or canal environment monitoring applications, and even the information collection application for Smart Grid.

This paper designs an information and energy-related IDS with hybrid mechanism for IoT applications with a path-constrained mobile sink. The hybrid IDS provides a trace-back mechanism for network forensics and enhances the network safety. The main contributions of this paper are summarized as follows:

Figure 1. Network threats and IDS categories


Network Threats
Unauthorized Access
Malicious Code
Service Interruption
Intrusion Detection Systems (IDS)
Distributed IDS
Hybrid IDS
Centralized IDS