


Sinkhole Attack Detection-Based SVM In Wireless Sensor Networks

Siheem Aissaoui, EEDIS Laboratory, Computer Science Departement, Djilali Liabes University of Sidi Bel Abbas, Algeria

Sofiane Boukli Hacene, EEDIS Laboratory, Computer Science Departement, Djilali Liabes University of Sidi Bel Abbas, Algeria

 <https://orcid.org/0000-0002-9760-3806>

ABSTRACT

Wireless sensor network is a special kind of ad hoc network characterized by high density, low mobility, and the use of a shared wireless medium. This last feature makes the network deployment easy; however, it is prone to various types of attacks such as sinkhole attack, sybil attack. Many researchers studied the effect of such attacks on the network performance and their detection. Classification techniques are some of the most used and effective methods to detect attacks in WSN. In this paper, the authors focus on sinkhole attack, which is one of the most destructive attacks in WSNs. The authors propose an intrusion detection system for sinkhole attack using support vector machines (SVM) on AODV routing protocol. In the different experiments, a special sinkhole dataset is used, and a comparison with previous techniques is done on the basis of detection accuracy. The results show the efficiency of the proposed approach.

KEYWORDS

AODV, Host IDS, Intrusion Detection System, Network IDS, Performance Evaluation, Sinkhole Attack, SVM, Wireless Sensors Network

1. INTRODUCTION

Wireless Sensor Networks (WSN) are spontaneous networks consisting of tens to several hundreds and sometimes thousands of nodes called sensors or motes. These nodes are dispersed in an environment called a collector field in order to perform autonomously three complementary tasks: to collect data (generally measurements of temperature, humidity, vibrations, radiation, etc.), to process them and finally to transmit these data to the base station via a radio circuit. Figure 1 illustrates WSN architecture.

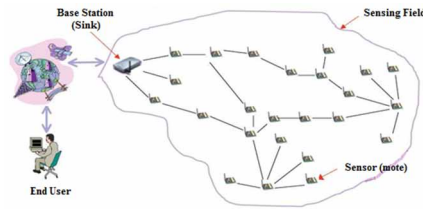
The attractive features of WSNs (small size, low cost, flexibility and facility of installation, large types of sensors, wireless communication) have enabled this type of networks to invade several application areas and be present not only in the industrial sector but also in medical and everyday life applications (García-Hernando et al. 2008).

Nodes in a wireless sensor network are typically deployed in hostile environments and left unattended with low computing, memory, and energy capabilities with vulnerable wireless communication that can be easily observed and interfered with. All those constraints make the WSN not only an easy target for several types of attacks but also make the application of the existing solutions for wired or even wireless systems inappropriate.

DOI: 10.4018/IJWNB.T.2021070102

Copyright © 2021, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Figure 1. Example of WSN architecture



Various types of attacks are possible on different layers of the sensor node and those that affect the overall performance of WSNs are known by denial of service attacks (dos). The first taxonomy of dos attacks for sensor networks has been discussed in (Wood and Stankovic 2002) and for whole attacks in (Roosta et al. 2006). The dos attacks on the routing protocols are the most attacks discussed in the literature (Karlof and Wagner 2003): sinkhole attack, blackhole attack, wormhole attack and selective forwarding attack. Therefore, a lot of solution has been proposed to improve security mechanisms for WSNs against dos routing attacks. Some related research are introduced and analyzed in following section.

In this paper, authors focus on sinkhole attack, which is one of the most destructive attack in WSNs (Ngai et al. 2006; Abdullah, et al. 2015; Raju and Parwekar 2016, Abdirahman and Sukhkirandeep 2019, Zhang and Liu 2019, Sejaphala and Velepini 2020). This attack consists to prevent the base station to receive packets from whole network by attracting all the traffic from neighboring nodes close to the base station based on fake routing information. WSNs are particularly vulnerable to sinkhole attacks due to the communication pattern “many to one” where sensor nodes route data to single base station. Sinkhole attack can be launched from a compromised node or a counterfeit node introduced inside the network. Once launched successfully, sinkhole node can be used to launch further attacks such as selective forwarding attack, wormhole attack, flooding attack, sybil attack and blackhole attack.

The objective of this work is to design and implement an efficient detection scheme based on SVM technique for intrusion detection system (ids) in WSN with energy saving (Lu et al. 2013) (Lu et al. 2014) (Lu et al. 2015). The proposed ids aims to detect a specific dos routing attack namely the sinkhole attack by using two routing information: hop count (HCNT) and destination sequence number (DSN) on ad hoc on demand distance vector (AODV) (Perkins et al. 2003) protocol. Authors experimented binary class support vector machines (SVM) to perform SVM classifier. The dataset used in different experimentations is provided by Garofalo and al in (Garofalo et al. 2013) for a comparison.

The remainder of this paper is organized as follows. Section 2 references related work for Sinkhole attack detection. Section 3 presents the existing attack datasets. Section 4 introduces SVM classification for intrusion detection. The obtained results are presented in section 5 and 6 and discuss in section 7. Finally paper concludes with section 8.

2. BACKGROUND AND RELATED WORK

In network security, Intrusion Detection Systems are considered as a second line of defense since attacks cannot be always avoided or prevented. IDSs already represent a key tool for ensuring cyber security in traditional computer based systems and they became an active research topic for wireless sensor networks.

The classification of intrusion detection systems depends on (1) the data collection mechanism (2) how attacks are detected (3) infrastructure (4) Sharing information (5) type of intrusion (6) Source of attack (7) frequency of use.

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/sinkhole-attack-detection-based-svm-in-wireless-sensor-networks/282471

Related Content

Enhancement of Network Performance in VANET Using Dynamic Routing Strategies

Mamata Rathand Sushruta Mishra (2021). *Managing Resources for Futuristic Wireless Networks* (pp. 266-291).

www.irma-international.org/chapter/enhancement-of-network-performance-in-vanet-using-dynamic-routing-strategies/262556

Integrating E-Learning 2.0 into Online Courses

Steve Chi-Yin Yuen (2016). *Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications* (pp. 1477-1488).

www.irma-international.org/chapter/integrating-e-learning-20-into-online-courses/138339

Intelligent Tracking and Positioning of Targets Using Passive Sensing Systems

Saad Iqbal, Usman Iqbal and Syed Ali Hassan (2019). *Next-Generation Wireless Networks Meet Advanced Machine Learning Applications* (pp. 286-305).

www.irma-international.org/chapter/intelligent-tracking-and-positioning-of-targets-using-passive-sensing-systems/221436

HTTP Traffic Model for Web2.0 and Future WebX.0

Vladimir Deartand Alexander Pilugin (2011). *International Journal of Wireless Networks and Broadband Technologies* (pp. 50-55).

www.irma-international.org/article/http-traffic-model-web2-future/53019

The Design and Modeling of 2.4 and 3.5 GHz MMIC PA

Chin Guek Ang (2012). *Advances in Monolithic Microwave Integrated Circuits for Wireless Systems: Modeling and Design Technologies* (pp. 105-156).

www.irma-international.org/chapter/design-modeling-ghz-mmhc/58490