Journal of VLSI Circuits and Systems, ISSN: 2582-1458 Vol. 4, No. 2, 2022 (pp. 1-4)

RESEARCH ARTICLE WWW.VLSIJOURNAL.COM

Design and Development of Intrusion Detection System for Wireless Sensor Network

Morukurthi Sreenivasu[1], Uppalapu Vinod Kumar[2], Ramesh Dhulipudi[3]

[1-3]*Department of Computer Science and Engineering, Godavari Institute of Engineering and Technology*

KEYWORDS:
Cluster, Intrusion detection, Rule-based detection Introduction, WSN.

ARTICLE HISTORY:
Received: 08.11.2021
Accepted: 21.01.2022
Published: 23.02.2022

DOI:
https://doi.org/10.31838/jvcs/04.02.01

Abstract

For various applications, wireless sensor networks are becoming more prevalent. It is necessary to prevent unauthorized access to sensor networks. This paper shows overview of WSN and intrusion detection methods. This paper proposed hybrid intrusion detection system (HIDS) for cluster WSN.

Author's e-mail: msreenivasucse@giet.ac.in, vinod.uppalapu@gmail.com, rameshdhulipudicse@giet.ac.in

How to cite this article: Sreenivasu M, Kumar UV, Dhulipudi R. Design and Development of Intrusion Detection System for Wireless Sensor Network. Journal of Complementary Research, Vol. 4, No. 2, 2022 (pp. 1-4).

Introduction

Security is a major issue that most protocol designers are addressing when it comes to implementing WSNs. Wireless sensor network is a type of network that uses a wide variety of small mobile devices equipped with sensors. Its features include: large-scale, self-organizing, multi-hop, and no-partition. Its price is lower than that of other similar devices. Security protocols are usually designed to protect a network from unauthorized access and exploitation. A security protocol should support various requirements related to network security. An effective security protocol can help prevent attacks before they happen. If they behave more actively in disrupting the network communications, they will cause some anomalies. An intrusion can be defined as an action that leads to unauthorized access to a wireless network. Usually, an inflow of suspicious activities can detect anomalous behavior. Intrusion detection systems are used to monitor a computer network for possible unauthorized access. [9],18], They then inform users about the detected activities.

Signature-based security systems measure the observed behavior of an attacker against known attack patterns. The system then stores these patterns in its database.[7] Intrusion detection systems have to be able to detect anomalous activities in order to prevent them from happening. An intrusion detection system can classify actions into three main categories: misuse detection, anomaly detection, and specification-based detection.

A misuse detection system measures the observed behavior of an individual or group of people. It is compared with known attacks patterns. Then, the system tries to identify the bad behavior based on these patterns. It avoids generating false positives by analyzing the behavior. It has been concluded that the memory constraints of ID systems make them less likely to be effective at storing attack signatures[6]. It uses behavior matching the known attack scenario to analyze the data in a network. It does so by comparing the information collected by the network to a large database. Anomaly detection systems are focused on identifying normal behaviors instead of attack vectors. They first flag any activities that are different from the norm. An anomaly detection technique is a type of security technique that focuses on the unusual behavior of a network. It can detect new types of attacks without requiring deep knowledge in network security.

A specification-based detection system is different from an attack detection system, which is based on deviations from normal operation. This technique is used for developing machine learning techniques that can detect normal behavior in sensor networks. It avoids the need for deep learning techniques and training. The remainder of this paper is organized as follows: Section II introduces the security issues and object to be detected in Wireless Sensor Networks. The existing methods of Intrusion Detection in Wireless Sensor Networks are discussed in Section III. In Section IV, existing methods are analyzed. The proposed model has discussed in Section V and concluded in Section VI.

Intrusion Detection in Wireless Sensor Network

Issues Related to Security

Aside from traditional network security problems, Wireless Sensor Network also faced many security issues such as active attacks, internal attacks, and external attacks. Attacks can be divided into several layers, which can be easily categorized as protocols. The goal is to create an intrusion detection framework that is compatible with the various requirements of WSN.

- The framework includes the following layers:
- The network layer refers to the section of the WSN that carries traffic between the sensor nodes and the network.
- Security ontology is a layer that refers to the formal semantics of security activities.
- The model layer is used for the single sensor node intrusion detection. The model takes into account the various behaviors of the sensor nodes.
- The cooperative layer is used for detecting intrusions. In this layer, we use a multi-agent system to cooperate with each other. Here we use a multi-agent system (MAS) to achieve the cooperation.

Object Detection

The objects of the WSN for intrusion detection mainly include the following:

- *Natural events:* Environmental variables (temperature, humidity), based on statistical methods of the data,[8] or using Hidden Model.[13]
- *System parameters:* Carrier sense time, signal strength, and packets delivery ratio.
- *Network data:* Network status information, such as routing table information, changing in neighbor nodes.
- *Custom parameters:* Malicious node, key etc.

Paper Existing Method of intrus detection

Rule-based

Rule-based intrusion detection[11] is a method used for monitoring network traffic and collecting data. The collected data are then placed in a queue. If the rules are satisfied, an intrusion is detected. The algorithm has three phases for detecting intrusions. In the first phase monitor nodes monitors the data. The first phase of the detection process is carried out in order to collect the necessary information to flag failure. The second phase is followed by the intrusion detection phase, which measures the number of failures that were flagged. The third phase of security is the intrusion detection phase, which is carried out when a high number of failures are detected. A message collision is a common occurrence that occurs when a message is sent and received over HTTP. Also, data alteration is a common occurrence when a message is sent and received over HTTPS.

Multi-Agent Based

In WSN, multi-agent distributed IDSs are used to improve the system's reliability and minimize the system's fault tolerance. The MAIDS uses the flexible programming of agents to achieve the various modules of the intrusion detection system. It saves money and is easy to implement. [12] The MAIDS is a multi-agent system that enables multiple intrusion detection units to communicate with each other as given in Fig. 1.

Data-mining based

Data mining techniques such as association rules, time series forecasting, and cluster mining are used to analyze and monitor the fusion data of the WSN[15]. Nuclear clustering is a technique to detect routing attacks caused by network traffic anomalies. It uses the latest technology to improve its detection accuracy and extend the time dimension.

Clusters-Based

Hierarchical WSN refers to the division of a network into various parts, such as head cluster and members of nodes. [16]. Through the cluster head, other members of the cluster relay information to each other.

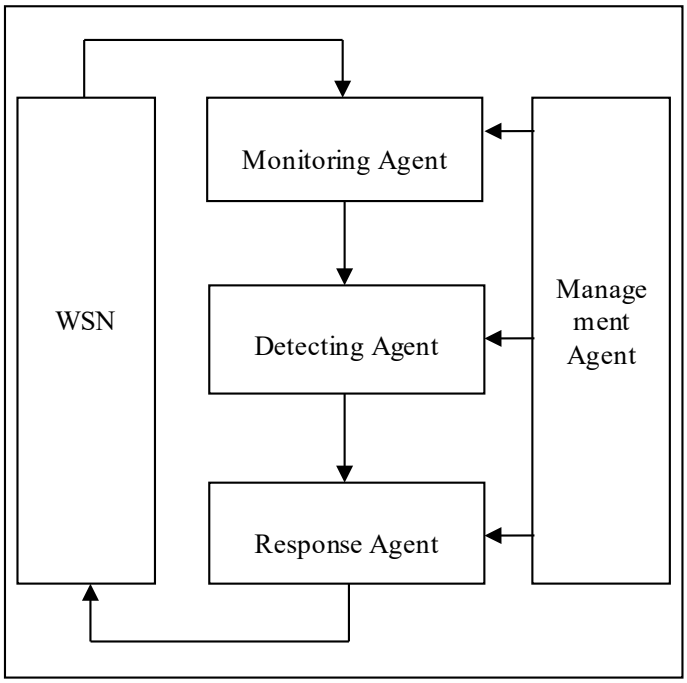

Fig. 1: The Structure of Multi-Agent Based

Artificial Immune Based

Paul Harmer proposed [10] an artificial immune system architecture for the modern internet network. Data collected from the normal conditions. Then, generate a random string collection to represent the most original "Detector" R0. The negative selection method compares the selected string to the matched R0 and then clears it. The "Detector" is activated when the network data matches the string of set R. If the frequency exceeds a threshold, the "detector" will be eliminated.

Hybrid Approach

The Hybrid approach combines the advantages of both the Cluster-Based and Rule-based techniques. This combination of high-speed, energy-efficient, and low-cost Intrusion Detection Systems makes it possible to provide high-quality, reliable, and secure solutions.

Analysis

Comparing analysis, for the advantages and disadvantages of different methods:

- Rule-based programming is a simple and effective method to solve security issues. However, it has disadvantages such as low security level.
- Multi-Agent Based method can reduce the network load and provide better security, but it also consumes a high amount of energy.
- Data mining is a technique that uses large amounts of collected data to detect anomalous attacks.
- The cluster-based method is more energy-efficient, but it has higher safety. It is also more complex, and its failure can affect the current network.
- Hybrid approach uses the principle of decreasing the amount of information in a network to increase the detection rate and the accuracy rate.

Proposed Model – HIDS for Cluster based Wireless Sensor Network

The proposed HIDS consists of two modules namely, intrusion detection and decision making. The latter provides a set of rules that are used to filter the packets sent by an attacker. This module can be used to take an action on a false Node.

Proposed System Architecture

The Hybrid Intrusion Detection Model is a proposed framework that can be used for cluster-based wireless sensor networks. It consists of two modules, which are shown in the figure 2. The Intrusion Detection Engine sends the incoming packets to the decision making module. The decision-making module uses the base station's predefined procedures to determine if an intrusion occurs.

We divide the network into groups, each of which has a cluster head (CH). The energy-efficient cluster heads are fixed and are responsible for the network's operation. The goal of a cluster-based routing system is to provide the longest possible life of the network. It does so by reducing the amount of data that the network consumes. Some of the Cluster-based routing protocols founded in the literature are: LEACH,[15], PEGASIS,[16] and HEED.[17]

Algorithm

In order to successfully implement Wireless Sensor Networks, one must first analyze and cluster the various algorithms involved in the design. These attributes are very important in wireless sensor networks. They include the cost of clustering, the selection of cluster heads, the operation of data aggregation, and the quality of service.

The concept of this paper is to divide the wireless sensor network into small groups, and to use a hierarchical clustering to divide the sensor nodes. This architecture is mainly used for monitoring industrial applications. After the Clustering process, the selected cluster head was dynamically selected according to the status of the nodes.

Usually, a cluster has the highest energy left over for a particular node. It is also required for large-scale ad-hoc deployments. Clustering cuts network contention by de-congestioning inter-cluster interference. Having multiple cluster heads can help conserve energy and reduce latency. It can also improve network reliability by pooling and aggregating data.

In a CWSN, it is necessary that the packets have normal patterns of behavior to monitor their status. This process involves the use of rules-based analysis to build an intrusion detection module. The modules are defined by experts.

The packets sent by the network members are analyzed using the history.

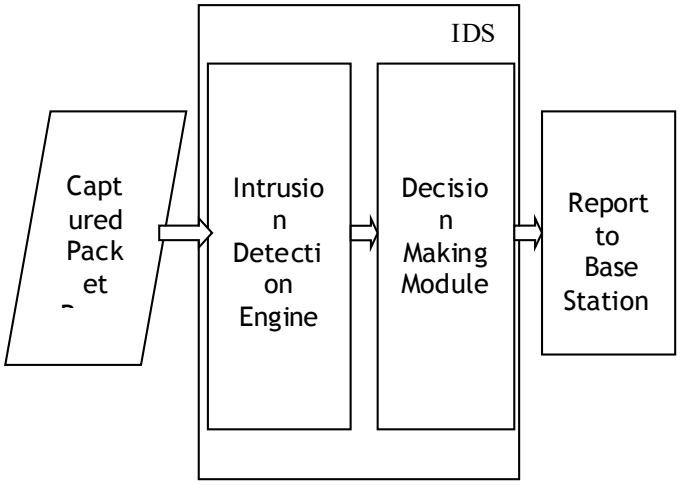

Fig. 2: The Proposed System Architecture

- **Step1:** The neighbor of CH is the transmission path of past packets. It is also the source of packet types that are analyzed.
- **Step2:** Features identification key features to distinguish between normal and abnormal packets.
- **Step 3:** The establishment of anomaly detection rules.

Conclusion

Various techniques are presented in this paper for detecting wireless sensor network intrusion. Insecurity detection in wireless sensor network can not solve all the problems that arise from it. For instance, high detection rate and low energy consumption are still not enough to protect inspection nodes safety. The proposed Hybrid Intrusion Detection Model would solve the above problems.

References

[1] Hichem Sedjelmaci and Mohammed Feham ,"Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor Network", IJNSA,Vol 3, No 4, July 2011.

[2] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Alaska, 11 May 2003, pp. 113-127.

[3] O. Younis, and S. Fahmy, "Heed: A hybrid, Energy-Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks", IEEE Transactions on Mobile Computing, vol.3, No.4, 2004, pp.366-379.

[4] S. Lindsey, and C. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information System", In Proc.IEEE Aerospace conference, vol.3, 2002, pp.1125-1130.

[5] W. R. Heinzelman, A. Chandrakasan , and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks", Proceeding of the 33rd Hawaii International Conference on System Sciences, IEEE, 2000, pp.1-10.

[6] A. Mishra, K. Nadkarni, and A. Patcha, "Intrusion detection in wireless ad hoc networks," IEEE Wireless Communications, vol. 11, no. 1, February 2004, pp. 48–60.

[7] S. Axelsson, "Intrusion detection systems: A survey and taxonomy," Department of Computer Engineering, Chalmers University of Technology, Tech. Rep. 99-15, March 2000.

[8] Shuai Liu, Jun-Jia Zhu and Ma Zhenyan, "wireless Sensor Network intrusion detection based on statistical anomalies(In Chinese)".

[9] R. Bace, "Intrusion Detection", MacMillan Technical Publishing, 2000.

[10] P. Harmer, P. Williams, G. Gunsch and G. Lamont, "AN artificial Immune System Architecture for Computer Security Applications", IEEE Transactions on Evolutionary Computation, Volume 6 issue 3, 2002, pp. 252-280.

[11] R.A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," Computer, 35(4), 2002, pp. 27-30.

[12] O. Kachirski and R. Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", IEEE Workshop on Knowledge Media Networking (KMN'02), Kyoto, JAPAN, 2002, pp 153-158.

[13] S. Doumit and D. P. Agrawal, "Self-organized Critically & stochastic learning based intrusion detection system for wireless sensor network", MILCOM2003-IEEE/ACM transactions on Networking, Vol. 11(1), 2003, pp 2-16.

[14] A. Paula, R. Da Silva, M. Martins and B. Roeha, "Decentralized Intrusion Detection in Wireless Sensor Networks", International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems Proceedings of First ACM International Workshop on Quality of Services and Security in Wireless and Mobile Networks, 2005, pp 16-23.

[15] Z. Jun, " Study on Several Issues in Wireless Sensor Networks Based on Data Mining", Shanghai Jiao tong University master thesis 2007(In Chinese).

[16] R. Chen, C. Hsieh and Y. Huang, "A new Method for Intrusion Detection on Hierarchical Wireless Sensor Networks", ACM ICUIMC- 09, Suwon, S. Korea, 2009.

[17] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection of Cluster-based Wireless Sensor Network", Proceedings of International Multi-Conference of Engineers and Computer Scientists , Hong Kong, Vol. 1, 2009.

[18] J. Zheng and A. Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEE, 2009.

[19] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network", Chayang University of Technology, Taiwan, IEEE 2010, pp. 114-118.