"STUDY OF SHIP INTRUSION DETECTION SYSTEM IN WIRELESS SENSOR NETWORK"

[1]KARTIK D. GORE
ME Scholar, Sanmati Engineering College, Washim, India
kartik11gore@gmail.com

[2]PROF SACHIN VYAWHARE
Assistant Professor, Sanmati Engineering College Washim, India
vyawhare999@rediffmail.com

ABSTRACT: *Monitoring is major problem for harbor protection, border control and security of various commercial facilities. It is challenging job to secure the sea areas and busy harbor areas from of unauthorized large ship or boat. Monitoring is very important to access information of every ship information such as speed and location. However, the speed and location of illegal ships are difficult to be gathered because they usually turn the Automatic Identification System signal off. In this paper present the study of intrusion detection system and also discuss the need of ship intrusion detection in wireless sensor network.*

***Keywords*:** ship intrusion detection, wireless sensor network, Automatic Identification System

1. INTRODUCTION

In recent years, advancements in computer and network technology have created the activity of using the internet an very important part of our daily life. Wireless Sensor Network (WSN) offers a wide range of applications in areas such as traffic monitoring, medical care, inhospitable terrain, robotic exploration, and agriculture surveillance. The advent of efficient wireless communications and advancement in electronics has enabled the development of low power, low cost, and multifunctional wireless sensor nodes that are characterized by miniaturization and integration. Intrusion detection system is used to detect unauthorized large ship or boat of harbor areas that can compromise the security or protecting the sea surface. In this paper present the study of intrusion detection system and also discuss the need of ship intrusion detection in wireless sensor network

2. LITERATURE REVIEW

Dr. Shashikant Dugad et. al. [1] presents a state-of-the-art solution for ship intrusion detection using image processing and Support Vector Machine (SVM). The main aim is to detect the ships, which cross over the border and secured industrial spaces. Using the interworking mechanisms of these two techniques, we can detect the intruding ship from the constantly changing sea environment. SVM can be used as a machine learning to train the system by exposing it to different seashore environments. Hence, it can be used as a real time security system at seashore areas.

Ajib Setyo Arifin et. al. [2] proposed location estimation using four numbers of sensors. They show model using graphical representations and easy see any conditions that may appear. Based on these conditions, derive formula by taking into account the diverging waves disturb sensors. When the diverging waves disturb the sensor, sensors create timestamps. Based on the difference of time stapms and characterize into three conditions, i.e. $t1 > t3$, $t1 < t3$, and $t1 = t3$. $t1 > t3$ means that the diverging waves arrive at sensor 3rd earlier than sensor 1st. $t1 < t3$ means that the diverging waves arrive at sensor 1st earlier than sensor 3rd. $t1 = t3$ means that the diverging waves arrive in sensor 1st and 3rd at same time. Using trigonometry and derive some intermediate step to compute x and y. they show that x and y are function of the timestamps and distance between sensor.

Ramandeep Kau et. al. [3] proposed model has been programmed for the detection of the intrusion attacks, which is observed from the intrusion pattern logs. The proposed model is a post analytical paradigm for the observation of the intrusion attack based intrusions out of the input data. The proposed model has been design with the amalgamation of the genetic algorithm and the SVM classification algorithm for the purpose of the intrusion attack detection. The genetic algorithm optimizes the data patterns observed as the intrusion attacks, which further undergoes the SVM classification for the final determination of the attacks. The proposed model has been recorded with the higher detection accuracy nearly at more than 99.46% in most of the rotations. The total 20 number of observations has been made before the final computation of the classification accuracy, where the proposed model has been recorded with the average classification accuracy of 92.09%. The proposed model has been good performance in the detection of U2R and R2L as compare to existing model.

Hanjiang Luo et. al. [4] present an innovative solution for ship intrusion detection. Equipped with three-axis accelerometer sensors, we deploy an experimental wireless sensor network on the sea surface to detect ships. Using signal processing techniques and cooperative signal processing, we can detect the passing ships by distinguishing the ship-generated waves and the ocean waves. We design an intrusion detection system

in which we propose to exploit spatial and temporal correlations of the intrusion to increase detection reliability. We conduct evaluations with real data collected by our initial experiments, and provide quantitative analysis on the detection system, such as the successful detection ratio and the estimation of the intruding ship velocity.

Lizhong Xiao et. al. [5] proposed alarm flooding, a hierarchical alarm processing model. The results of simulations show that it has satisfying detection rate and false alarm rate for attacks, high compression rate for alarms and high accuracy for alarm correlation. However, an intrusion can be detected by several sensors, so some alerts collected by controller from the distributed sensors are reported about the same intrusion.

3. INTRUSION DETECTION SYSTEM

An intrusion detection system is one of the types of security software system designed to automatically aware the administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

An IDS works by monitoring system activity through examining vulnerabilities in the system, the integrity of files and conducting an analysis of patterns based on already known attacks. It also automatically monitors the Internet to search for any of the latest threats which could result in a future attack.

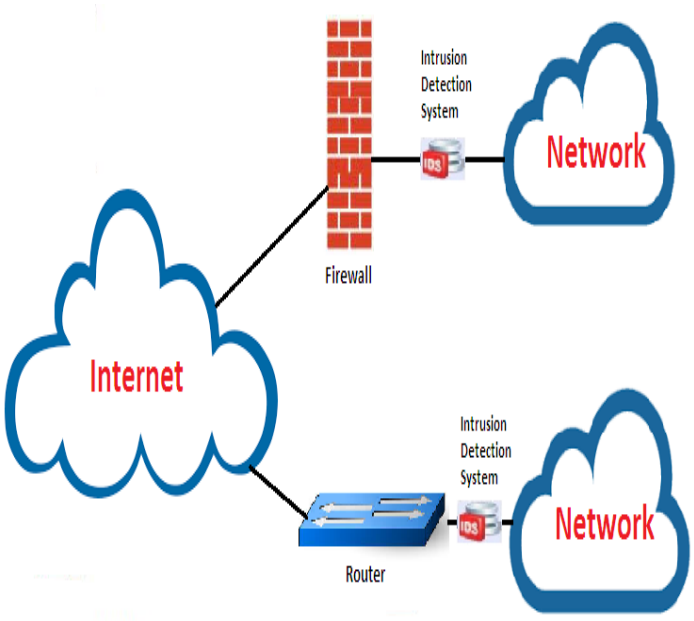

Figure 1: Intrusion Detection System

4. NEED OF SHIP INTRUSION DETECTION IN WIRELESS SENSOR NETWORKS

- Using the traditional method of detecting ships is with radars or satellites which are very expensive.
- High cost i.e. the satellite image is easily affected by the cloud.
- It is very difficult to detect small boats or ships on the sea with marine radar due to the noise or clutters generated by the uneven sea surface.
- Energy loss due to data transmission.

5. CHALLENGES OF INTRUSION DETECTION

Intrusion detection systems in theory looks like a defense tool which every organization needs. However there are some challenges the organizations face while deploying an intrusion detection system. These are discussed below.

1. IDS technology itself is undergoing a lot of enhancements. It is therefore very important for organizations to clearly define their expectations from the IDS implementation. IDS technology has not reached a level where it does not require human intervention. Of course today's IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable period of time, dynamically modifying a router's access control list in order to stop a malicious connection etc.

2. The success of an IDS implementation depends to a large extent on how it has been deployed. A lot of plan is required in the design as well as the implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS to benefit from both. In fact one technology complements the other. However, this decision can vary from one organization to another. A network based IDS is an immediate choice for many organizations because of its ability to monitor multiple systems and also the fact that it does not require a software to be loaded on a production system unlike host based IDS.

3. It is important to take care of sensor to manager ratio. There is no thumb rule as such for calculating this ratio. To a large extent it depends upon how many different kinds of traffic is being monitored by each sensor and in what environment.

4. The IDS technology is still reactive rather than proactive. The IDS technology works on attack signatures. Attack signatures are attack patterns of previous attacks. The signature database needs to be updated whenever a different kind of attack is detected and the fix for the same is available. The frequency of signature update varies from vendor to vendor.

5. While deploying a network based IDS solution, it is important to keep in mind one very important aspect of the

network based IDS in switched environment. Unlike a HUB based network, where a host on one port can see traffic in and out of every other port in the HUB, in a switched network however, traffic in and out of one port cannot be seen by a host in another port, because they are in different collision domains.

6. REFERENCES

[1] Dr. Shashikant Dugad, Vijayalakshmi Puliyadi, Heet Palod, Nidhi Johnson, Simran Rajput, Swapna Johnny, "Ship Intrusion Detection Security System Using Image Processing & SVM", International Conference on Nascent Technologies in the Engineering Field (ICNTE-2017), 2017.

[2] Ajib Setyo Arifin, Teguh Samudra Firdaus, "Ship Location Detection Using Wireless Sensor Networks with Cooperative Nodes", IEEE, 978-1-5090-4749-9/17/$31.00 ©2017.

[3] Ramandeep Kaur Meenakshi Bansal, "Multidimensional Attacks Classification Based on Genetic Algorithm and SVM", 2nd International Conference on Next Generation Computing Technologies (NGCT-2016), Dehradun, India 14-16 October 2016.

[4] Hanjiang Luo, Kaishun Wu, Zhongwen Guo, Lin Gu, Zhong Yang,Lionel M. Ni, "SID: Ship Intrusion Detection with Wireless Sensor Networks", 31st International Conference on Distributed Computing Systems, 2011.

[5] Lizhong Xiao, Yunxiang Liu, Lizhong Xiao, Lizhong Xiao, Zhongdai Wu, "A Hierarchical Alarm Processing Model for Intrusion Detection System",

[6] Arivazhagan.B, Shyam Sundhar.B B, "Advanced Border Intrusion Ship Detection using Wireless Sensor Networks", International Journal of Advanced Research in Electronics, Communication & Instrumentation Engineering and Development Volume: 2 Issue: 2 26-Jun-2014.

[7] Sathish Babu Nr, Aravind Swaminathan G, D. C. Joy Winnie Wise, "Ship Detection and Surveillance with ENS_ORA using Wireless Sensor Networks", International Journal On Advanced Computer Theory And Engineering (IJACTE), Volume -4, Issue -6, 2015.

7. AUTHOR PROFILE

Kartik D. Gore completed Bachelor of Engineering in Computer Science and Engineering from Sanmati Engineering College, Washim and pursuing Master of Engineering in Computer Science and Information Technology from Sanmati Engineering College, Washim, India

Prof. Sachin Vyawhare is working as Asst. Professor and HOD of Computer Department at Sanmati Engineering College Washim (MH). He received BE degree and ME degree from S.G.B.A.U. Amaravati. His research interest includes networking, Operating System and Image Processing.