

International university of malaya-wales

bachelor of computer science

BCS 504 – Project 1

Muhammad Ibrahim Khalil ID-201701249

**Contents**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **Section 1** | **Introduction** |  |
| 1.1 | Overview |  |
| 1.2 | Aim |  |
| 1.3 | Objectives |  |
| 1.4 | Problem statement |  |
| 1.5 | Research |  |
| 1.6 | Significance of the project |  |
| 1.7 | Limitations of the project |  |
| 1.8 | Organization of the report |  |
| 1.9 | Conclusion |  |
| **Section 2** | **Literature Review** |  |
| **Section 3** | **Research Methodology** |  |
| **Section 4** | **Requirement Analysis Selection of tools, techniques, and methods** |  |
| **Section 5** | **Design & Development** |  |
| **Section 6** | **Evaluation** |  |
| **Section 7** | **Conclusion** |  |
| **Section 8** | **Links and References** |  |
| **Section 9** | **Log Sheet** |  |
| **Section 10** | **Index & Appendices** |  |

**Introduction**

An intrusion detection system or IDS is a hardware appliance or software application that use to monitors network traffic or package moving in any kind of networks to search for suspicious activities and unknown threats, sending up alerts when it that kind of threats item in the network.

Security is the major issue for the wireless and Mobile AD HOC network because it is using “AIR” as media. Research project address this part as Intrusion Detection. Mounting world cannot imagine even for a single day without computer and computer is basis on internet. Nowadays secure information of internet is becoming very high priority. Modern world emphases in a way by which it can be protect the data and information from any illicit and unauthorized access.

Currently, if Internet infrastructure assault such as man in the middle attack, denial of service attacks and worm’s infection, have become one of the most serious threats to the network security [1]. It is very likely feasible to detect the attacks and abnormal behaviors if there is sufficient and efficient method and technique exists for monitor and examine, and it can not only make sure proceed warning of potential attacks, but also help out to recognize the reasons, source and locations of the anomalies. By this way, it may assist to restrain the attacks, sooner than they have enough time to broadcast across the network. This document represents the method, in support of detecting network anomalies by analyzing the unexpected change of time series data. With the comparison of other anomaly detection methods. We have focal point on the vibrant behavior of the network rather than using the static models. Our process and method concern the Auto-Regressive (AR) process to model the rapid and unexpected change of time series data, and performs sequential hypothesis test in contrast with two adjoining non-overlapping windows of the time series to detect the anomalies

**1.1 Overview**

Intrusion Detection Systems (IDS) can be differs in various techniques and advance with the objective to detect suspicious traffic in dissimilar ways. There are two significant categories of intrusion detection systems. One is called network-based intrusion detection system (NIDS) and the other one is host-based intrusion system (HIDS). The existing system that detects attacks based on looking for specific signature of identified threats. It reveals particularly that we may have two sets of data; one is of usual and common data and other one apprehensive and suspicious data. So, intrusion detection systems match the data with the set of normal and suspicious data and if the deference between the two set is above a threshold value then intrusion is detected.

**1.2 Aim**

The aim of this thesis is to design and implement a IDS for wireless network to detect and monitoring malicious activities by using time series analysis techniques.

* Review current intrusion detection system
* Analyze the data with suspicious activities
* Design appropriate system architecture for IDS
* Implement the system using time series analysis
* Testing and evaluate the system.
* Future work

**1.3 Objectives**

* Identify the components of an intrusion detection and preventing system
* Describe options for implementing intrusion detection and prevention systems
* State the function of an Intrusion Detection System (IDS)
* Evaluate exterior and interior sensor placement effectiveness
* Consider trade-offs that influence exterior IDS design effectiveness

**1.4 Problem statement**

How to enhance existing WLAN intrusion detection system to efficiently identify serious attacks in wireless networks with fast learning and classification speed and high detection accuracy?

Each and every one carrying more than one device that devices connected to the network most of the time. so, these devices are connected with the network making it creating lots of volumes as traffic in a network data. this network data need to has to be monitored for some kind of thread. so, this dataset should be monitor find the thread or problem in the network data. because this traffic data needs to analyze to identify the thread as initial of defense. so that we can avoid bigger attack or bigger thread going to come to the networks. However, the existing technic is available but this technic is facing the challenges because of varieties of data that coming in and there facing challenges in their architecture is not supporting this one that's the mean challenges that we are facing with it. Meanly here we are focusing at the Linux base system. every time the Linux script also changing Linux sophisticated so the attack generated more for the Linux oriented network. overall the existing approach in a network monitoring is really facing an issue.

**1.5 Research questions**

In the present work an improved **hybrid wireless intrusion detection system (HWIDS)** is developed to address the research question:

1. How dose HWIDS compare to other published intrusion detection approaches in terms of precision and recall?
2. Can HWIDS detect attack in real-world wireless LANs and how fast is it?
3. How does HWIDS compare to other commercial intrusion detection systems (IDS)?
4. Evaluate and test the proposed solution for performance and efficiency.
5. Review and understand different types if WLAN attack

**1.6 Significance of the project**

This project seeks to assist in the understanding of intrusion detection system (IDS) and intrusion prevention system (IPS) technologies and in designing, implementing, configuring, securing, monitoring, and maintaining intrusion detection and prevention systems (IDPS). The project also provides an overview of complementary technologies that can detect intrusions, such as security information and event management software and network forensic analysis tools. It focuses on enterprise IDPS solutions, but most of the information in the project is also applicable to standalone and small-scale IDPS deployments.

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of attacks and secures the networks. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before.

**1.7 Limitations of the project**

Some of the major limitations during the course of the study were as follows;

* Financial constraint to provide adequate funding for the research
* Reluctance of some firms to provide information pertaining to the IDPS technologies they use
* Poor network reception for online research.
* Short time duration provided for the research.

**1.8 Organization of the report**

**1.9 Conclusion**

* Intrusion detection system are helpful enough that those who care about security should use them
* Improved the classification accuracy and speed