Network Intrusion Detection in Wireless Network using Kabsch Algorithm

N. Isbudeen¹, Syed Ajaz², Peer Ahamed Buhari³

Department of Information Technology
College of Computers and Information Technology, Taif University, Saudi Arabia

isbudeen@tu.edu.sa, u.ajaz@tu.edu.sa, buhari.m@tu.edu.sa

Abstract—A prototype implementation of a wireless network intrusion detection using Kabsch algorithm in order to implement a system that has ability to actively prevent the identified threats. The goal of intrusion detection is to identify misuse of computer systems by internal and external penetrators [3]. We propose a partitioning approach to network security analysis that support in depth, network intrusion detection in wireless network. Due to the variety of network behaviors and the rapid development of attack fashion [9]. It is necessary to develop machine learning based wireless network intrusion detection algorithm, in correspondence, we propose an intrusion detection algorithm based on the kabsch algorithm [8]. We demonstrate that high attack detection accuracy can be achieved by using digital matrix fields by implementing the Kabsch algorithm. This paper describes a new technique for monitoring and detecting security breaches that occurs in WLAN protocols. This research has also shown a methodology for configuration management assurance of an organization’s wireless router; this is key point of intrusion detection system, as improperly configured routers are the most dangerous risk of the WLAN [14]. This system presented along with conclusion as to what is necessary to implement as a more desirable and capable wireless intrusion detection.

Keywords—Intrusion detection, Wireless network, Network security analysis, Kabsch algorithm.

I. INTRODUCTION

In computer networks, computers are exposed to be attacked by external intruder. Many computer networks have been attacked against by their secured information; Intrusion detection has been an active field of research for about two decades, starting in 1980 with the publication of John Anderson’s “computer security threat monitoring and surveillance” which was one of the earliest papers in this field [10][11]. Intrusion detection is crucial part of network security, only if intrusion is correctly detected, sub- sequent process and recovery is implemented [1]. The goal of intrusion detection is to identify entities attempting to subvert in place of security controls. Most wireless networks communicate with layer 1 and 2 type of protocols designed by IEEE 802.11 group; these are various specifications which increase the communication speed by changing the frequency band. Standard tools for monitoring wired network and ensuring their security examine only network layer 3 the assumption that the lower layers are protected by physical security of the wires. However, this assumption cannot be exploding to wireless networks because of the broad cost nature [14]. Ideally, intrusion detection for wireless networks should function at the data link layer if high security is required, the wireless network intrusion detection offers intelligent protection of computer networks much better than using fixed firewalls. The design philosophy of this model is quiet different and it was rarely messed up with existing methods. In this paper, we represent a new digital matrix wireless intrusion detection system.

This system combines the positive features of intrusion detection to achieve higher detection accuracy, lower false alarm [12]. Our Intrusion detection method is network based which should not be confused by host-based intrusion detection abbreviation by other authors. We have taken existing 802.11 g digital matrix and explored what electronic methods may be employed for wireless attacks to minimize or prevent security. Kabsch algorithm recognizes attacks as well as for countering host attacks being explored [13]. An experimental explanation prototype which is limited proof of concept functionality, we discuss the related work with emphasis on various methods and framework for intrusion detection, and we describe the use of conditional digital matrix for intrusion detection. This paper presents as a wireless intrusion detection analysis and tool based on this approach, the algorithm is useful for the network traffic portion of manageable matrix size. The algorithm approach presents section III after discussion of related work in section II, section IV presents’ results of experiments of the tools, section V presents conclusions and section VI outlines of future work [9].

II. RELATED WORKS

Research for the new intrusion detection techniques is very important, since in everyday, new challenge of security appears for IT people and to make it hard to protect their network, researcher still try to increase percentage of intrusion detection accuracy in case of false to hit his ratio, another common attack is MAC address masquerading. In this attack wireless users sniff to determine the MAC addresses that are being allowed access to a wireless network [14]. Signal from wireless networks are usually multi directional beyond the coverage area, the most common wireless method is...
“Wardriving”, this is actually done using a Windows laptop running Wardriving software, such as Netstumbler and equipped with IEEE 802.11b adopter. A different method was demonstrated by 802.11 Ninja during DefCon in 2007, using a program called Monkey-Jack, management frames were sent to wireless clients at the convention forcing them to disconnect from the valid APs and re associate instead with a bogus AP managed by the attackers. The attackers also often code their website to exploit other vulnerabilities even in wireless Virtual Private Networks; all these rely on unauthenticated message vulnerabilities on IEEE 802.11 networks [13]. Qin and Wang refined the rule formulation procedure with an adaptive based support algorithm to mine normal traffic records [9].

In this paper, we propose the wireless network intrusion detection architecture and prove its effectiveness through simulation experiments; the wireless network intrusion detection indicates the flexibility of intrusion detection system with the accuracy of Kabsch based intrusion detection. In this field number of methods and frameworks has been proposed many systems have been built to detect intrusion. Various techniques such as association rules, clustering, naïve Bayes classifier, support vector machine, genetic algorithm, artificial neural networks and other have been applied to detect intrusion. The possibility of performing wireless network based intrusion detection on wireless networks has been the focus of much debate in the intrusion detection community. A common position is to state that wireless network intrusion detection is not practical because of the technical difficulties encountered in keeping pace with the increasing network speed and the more widespread use of encrypted traffic [8]. Very few research papers have been published that deal with the problem of intrusion detection on wireless networks. We reviewed the related work, focusing on the types of algorithm that are described in the literature. Denning proposes a statistical method for intrusion detection. According to audit data, a profile is constructed to describe a given subject or a given task. The Gaussian models of the metrics are constructed to detect intrusions. Li et al [9]. utilize statistical characteristic of n-grams to detect intrusion in the host system. Vigna and Kemmerer use data that are sourced from the network nodes, rather than the audit data to construct profiles, enlightening the research on network based intrusion detection [9].

III. OVERVIEW OF KABSCH ALGORITHM

A. Description

The algorithm starts with two sets of paired points, P and Q. Each set of points can be represented as an \( N \times 3 \) matrix. The first row is the coordinates of the first point, the second row is the coordinates of the second point, the \( N^{th} \) row is the coordinates of the \( N^{th} \) point.

\[
\begin{pmatrix}
x_1 & y_1 & z_1 \\
x_2 & y_2 & z_2 \\
\vdots & \vdots & \vdots \\
x_N & y_N & z_N \\
\end{pmatrix}
\]  

(1)

The algorithm works in three steps: a translation, the computation of a covariance matrix, and the computation of the optimal rotation matrix.

B. Translation

Both sets of coordinates must be translated first, so that their centroid coincides with the origin of the coordinate system. This is done by subtracting from the point coordinates the coordinates of the respective centroid.

C. Computation of the covariance matrix

The second step consists of calculating a covariance matrix \( A \). In matrix notation,

\[
A = P^TQ
\]  

(2)

or, using summation notation,

\[
A_{ij} = \sum P_{ki} Q_{kj}
\]  

(3)

D. Computation of the optimal rotation matrix

It is possible to calculate the optimal rotation \( U \) based on the matrix formula \( U = (A^T A)^{1/2} A^{-1} \) but implementing a numerical solution to this formula becomes complicated when all special cases are accounted for (for example, the case of \( A \) not having an inverse).

If singular value decomposition (SVD) routines are available, the optimal rotation, \( U \), can be calculated using the following simple algorithm.

First, calculate the SVD of the covariance matrix \( A \).

\[
A = V S W^T
\]  

(4)

Next, decide whether we need to correct our rotation matrix to insure a right-handed coordinate system

\[
d = \text{sign} (\det(A))
\]  

(5)

Finally, calculate our optimal rotation matrix, \( U \), as...
IV. WIRELESS NETWORK INTRUSION DETECTION APPROACH

The overall goal is to perform wireless network intrusion detection analysis in wireless network using digital matrix in Kabsch algorithm.

1) System architecture

The requirement basis of Intrusion detection for the design based on wireless network, to solve this problem, we use connection sequence numbers to destinations, the first step is to filter out the known MAC address PC’s using Airsnare to determine the IP address to use for traffic control. The most common way people approach network intrusion detection is to detect statistical anomalies. The idea behind this approach is to measure a "baseline" of such states as CPU utilization, disk activity, user logins, file activity, and so forth. Then, the system can trigger when there is a deviation from this baseline.

![Diagram of Intrusion detection for wireless networks using digital matrix](image)

2) Evaluation and Results

Given this notation relative to the centroid, we can explicitly set the centroids to be equal and proceed with the rotational part of the alignment.

2.1) Computation of the covariance matrix

The second step consists of calculating a covariance matrix A. In matrix notation,

\[ \mathbf{A} = \mathbf{P}^T\mathbf{Q} \]  

(7)

or, using summation notation,

\[ A_{ij} = \sum_{k} p_{ik} q_{kj} \]  

(8)

This result can be confirmed by carrying out long multiplication of p and q. There is no analog in vector arithmetic for quaternion multiplication.

2.2) Optimal rotation matrix

Where \( d = \text{sign} \left( \det(C) \right) \).

In the light of the preceding derivation, all the facts that have been presented as a proof can be succinctly put as an algorithm for computing the optimal rotation to align two data sets x and y:

Build the 3xN matrices X and Y containing, for the sets x and y respectively, the coordinates for each of the N atoms after centering the atoms by subtracting the centroids.

Compute the covariance matrix \( \mathbf{C} = \mathbf{X} \mathbf{Y}^T \)  

(10)

Compute the SVD (Singular Value Decomposition) of \( \mathbf{C} = \mathbf{V} \mathbf{S} \mathbf{W}^T \)  

Compute \( d = \text{sign} \left( \det(C) \right) \)  

(11)

Compute the optimal rotation U as

Finally, calculate our optimal rotation matrix, U, as

Then the second largest value occurs when \( T_{11} = T_{22} = +1 \) and \( T_{33} = -1 \). Now, we have that \( T \) cannot be the identity matrix as before, but instead it has the lower-right corner set to -1. Now we finally have a unified way to represent the solution. If \( \det(C) > 0 \), \( T \) is the identity; otherwise, it has a -1 as its last element. Finally, these facts can be expressed in a single formula for the optimal rotation \( U \) by stating:

\[
U = W \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & d \end{pmatrix} V^T
\]

(12)

We set the number of values in DHCP to determine the IP address so we calculate loss of packets for each PC through MAC addresses also verify the MAC address figure 1 shows the applied digital matrix in Kabsch algorithm to detect intrusion in wireless networks.
Figure 2 determines Digital matrix applied Airsnare software to display MAC and IP address on complete network.

Figure 3 Alert of alarm digital matrix Air horn

AirSnare will alert you to unfriendly MAC addresses on your network and will also alert you to DHCP requests taking place. If AirSnare detects an unfriendly MAC address you have the option of tracking the MAC address's access to IP addresses and ports or by launching Ethereal upon detection.

When AirSnare detects a MAC address on the network that isn't listed in the Friendly MAC list, it will sound an alert and change the background screen color to red. At this point any traffic sent from that MAC address to the network will be logged in the Unfriendly MAC Watch Window (see to the top right). At this point you need to determine if the MAC address really is Unfriendly or if you just perhaps missed a device on your network somewhere.

Figure 4 view the visited Host IP address

This is where you can find out what the unfriendly MAC is up to. It will show you the source and destination IP address they are going to and the Source and Destination MAC Address. It will also identify common ports such as FTP, Telnet, e-mail, web, DHCP and other popular ports.

Figure 5 Graph of Packet losses due to the network traffic

Stateful monitoring of traffic could provide clues about intrusions this technique may be extended to the IEEE 802.11 b protocol on events.
It delivers the acknowledgement of the connectivity of each node to router it prevent unfriendly MAC address Traffic consists of IP datagram flowing across a network. Wireless network intrusion detection is able to capture those packets as they flow by on the wire. Wireless network intrusion detection consists of a special TCP/IP stack that reassembles IP datagram and TCP streams.

V. CONCLUSION

This paper presents the design and implementation of wireless network Intrusion detection, the evaluation of kabsch algorithm determines to monitor the attacks using Airsnare software, we summarize major contribution and make further work, the software successfully detecting the network intrusion in wireless network, the main advantage of our algorithm to examine the traffic from one channel to other channel.

VI. FUTURE WORK

For future work, we suggest the following issues in digital matrix using Kabsch algorithm for disabled port of the network, for future the current prototype for the further development, we will find new types of attacks in wireless network

ACKNOWLEDGEMENT

The intrusion detection system research and development authors sincerely thank the anonymous reviewers whose comments greatly helped clarify and improve this paper.

REFERENCES