Designing of Intrusion Detection System Based on Image Block Matching

Abdullah A. Mohamed and Dia M. Ali

Abstract—The Intrusion Detection System (IDS) is one of the most important network security systems. In this paper a new method is used to design off-line intrusion detection system, Simulink Image Block Matching and Embedded Matlab Function are used in the designing. The used method is very simple and efficient. The Image Block Matching is used for pattern matching and the Embedded Matlab Function is used for giving the decision. Three types of attacks are used in this paper (R2L, DoS and U2R). The result shows that the IBM can give a high detection and classification rate in average equal to 94.9 percent based on NSL KDD recorders.

Index Terms—Intrusion detection system, anomaly, artificial neural network, image block matching.

I. INTRODUCTION

Today, making connection between numbers of points is not enough to be a network unless, it be secured. The network security became one of the most important network’s factors, now, companies, banks and government offices need to communicate between the center office and the sub-offices and this communication need to be secured for that many types of networks security systems had been generated IDS, Intrusion Detection and Preventing System (IDPS) and Firewalls. IDS is a security system focus on the attacks that come from the inside of the network [1]. When we classify the designing of the IDS according to the real-time property, there are two types online and off line IDS system, on line IDS deals with the Ethernet in real time and it analyses the Ethernet packet and applies it on the some rules to decide if it an attack or not. Off line IDS deals with stored data and pass it on some process to decide if it an attack or not. Off line IDS deals with stored data and pass it on some process to decide if it an attack or not. Off line IDS deals with stored data and pass it on some process to decide if it an attack or not. Due to the fact that buildings are often under attack, they need to be protected.

II. RELATED WORKS


III. IMAGE BLOCK MATCHING (IBM)

Block Matching is one of the most powerful tools of Video and Image Processing Blockset in SIMULINK program Fig. 1 (a). It is used to match between tow images or to video frames. You can choose the mode of matching for tow images or the current frame and the N-the frame back from the block parameters window Fig. 1 (b). The work of this tool based on subdividing the image or the frame to a number of sub-blocks of pixels you entered in Block Size [height, width] and overlap [height, width]...
parameters Fig. 2. So by moving the block of pixel in the frame \( k \) over a search region in the block of pixel in the frame \( k+1 \) which is limited by Maximum displacement \([\text{height, width}]\) parameter, the mismatching can be computed as a mean square error.

![Image](https://example.com/image1.png)

Fig. 2. The work Technique of the IBM [3]

![Image](https://example.com/image2.png)

Fig. 3. IDS by using IBM

### IV. THE PROPOSED METHOD

Block Matching block is the proposed method for the designing. In this method we focused on two features of the Block Matching, the ability to estimate the motion between two images or two video frames and the ability to give the mean square errors between two images or two video frames, estimation, that mean the ability to generalize from incomplete data, mean square error that mean the ability to classify the data as normal or abnormal (attack). There are two ways to apply the IDS on the IBM as shown in Fig. 3. The first is to form the testing data as a two dimensions matrix and pass it to sub-matrix block according to the size of the testing records, then it pass to the IBM as image under test with another image formed from matrix which is taken from training data, the matching result will appear as matrix of mean square error, this errors is passed to Embedded Matlab Function to give the decision if it attack case or not.

The second method is to generate a video file from the testing data and the patch data that is tacked from the training records then it passed to the IBM and the other steps is the same of the first method, this method is more complicated from the first method, but it more faster than the first because of the reducing in the blocks, it became not stable as the testing records increases so we don’t recommend to use it.

### V. RESULTS AND CONCLUSIONS

In this section the designing results are produced. We used 1500 testing patterns for three classes of attacks (R2L, DoS and U2R) with 500 patterns for each class; the type of the used testing dataset is NSL-KDD. The results are produced as percentage values of successful classifications (PSC) on test dataset.

\[
PSC = \frac{\text{number of correctly classified instance}}{\text{number of instance in the test dataset}}
\]

We get PSC for R2L 93.8%, DoS 96.3% and U2R 94.6%, the average classification rate was 94.9 as shown in Table I.

### TABLE I: COMPARISON OUR RESULTS WITH OTHER WORKS

<table>
<thead>
<tr>
<th>Owner</th>
<th>Used method</th>
<th>Database</th>
<th>Result PSC %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vaitsekhovich</td>
<td>RNN &amp; MLP</td>
<td>KDD-99</td>
<td>85.59 94.2 86.54 88.77</td>
</tr>
<tr>
<td>Laheeb</td>
<td>DTDNN</td>
<td>KDD-99</td>
<td>95.8 97.6 96.2 96.53</td>
</tr>
<tr>
<td>Proposed</td>
<td>IBM</td>
<td>NSL-KDD</td>
<td>93.8 96.3 94.6 94.9</td>
</tr>
</tbody>
</table>

We can see that our results approached to the Laheeb’s results, but we used NSL-KDD database, it is more sensitive than KDD-99 and need high accuracy to get right classification. The results show that the IBM is suitable to be the base for classification applications and it doesn’t need training fuse just simple initialization fuse to determine the acceptable error in the classification.

### REFERENCES


Abdullah Abdulaziz Mohamed was born in Mosul-Iraq in 1988. He received his engineering degree in Communication Science from the University of Mosul in 2011. He is a student in master study of network security since 2011 till now.