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 there are standard data include most of the well-known attacks and it consist of two parts training data and testing data, these standard data like DARPA, KDD99 and NSL KDD include cases for the Ethernet Frame and it focused on some features in the frame, according to these cases it decide if it is an attack or normal frame. NSL KDD is a developed virgin of KDD 99 and it include 41 features[2], pattern matching for each record in the training and testing data can give the right decision and that which make the IBM suitable to chive this job, because it very efficient in pattern matching.

Manuscript received January 9, 2013; received March 13, 2013.

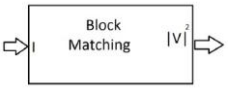
Abdullah A. Mohamed is with the Communication Department, Collages of Electronics Engineering-Mosul university-Iraq (e-mail: Abdullah.4Mohamed@Gmail.com).

Dia M. Ali is with College of Elec., Ninawa University, Ninawa, Iraq (e-mail: dia_mohanad@yahoo.com).

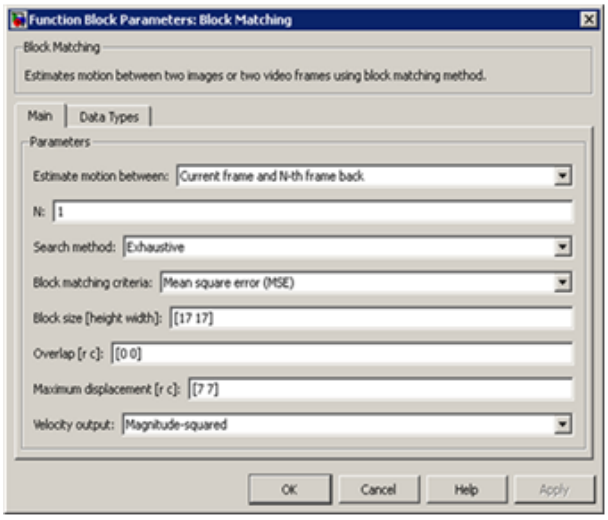
II. Related Works

In the recent ten years ago there were many of papers take about the designing IDS most of them used genetic algorithms and neural networks in the designing, Mukkamala S. (2002) produce a method to designing an IDS by using neural networks and support vector machine [4]. Moradi M. and Zulkernine M. (2004) used A Neural Network [5]. A. Morteza, R. Jalili and R. S. Hamid (2006) used unsupervised neural networks [6].T. P. Tran, L. Cao, D. Tran and C. D. Nguyen (2009) used probabilistic neural network [7]. M. Laheeb (2010) used Distributed Time-Delay Artificial Neural Network [8]. Shahbaa A. and Karam M. (2012) used hybrid intelligence system to design an IDS [9].

III. Image Block Matching (IBM)



(a). Block Matching



(b). Parameter Setting

Fig. 1. Image Block Matching [3]

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]

DOI: 10.7763/IJCCE.2013.V2.258

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 [height, width] parameter, the mismatching can be computed as a mean square error.

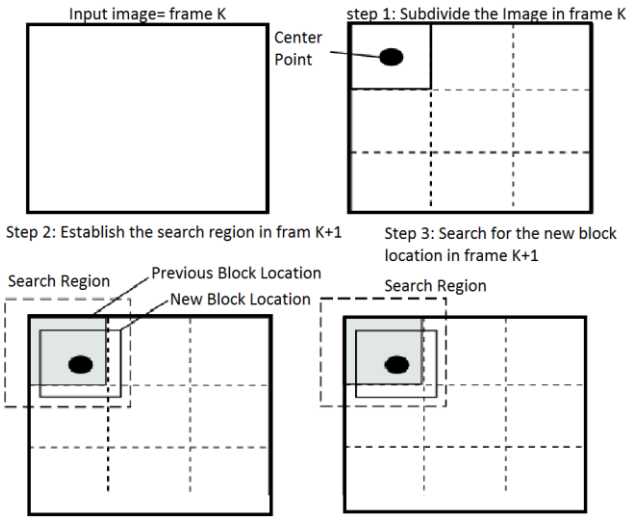


Fig. 2. The work Technique of the IBM [3]

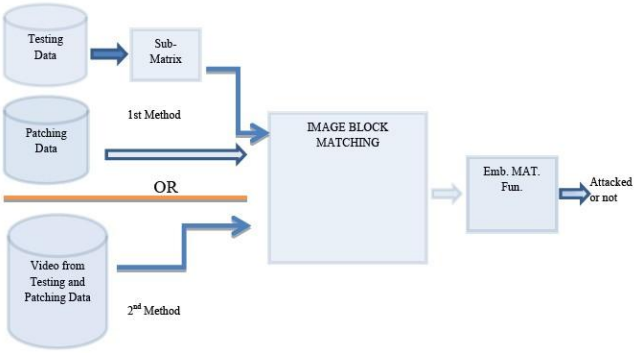


Fig. 3. IDS by using IBM

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 anther 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=(number of correctly classified instance / 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

Owner	Used method	Database	Result PSC %			
			R2L	DoS	U2R	AVG
Vaitsek-hovich [10]	RNN & MLP	KDD-99	85.59	94.2	86.54	88.77
Laheeb [8]	DTDNN	KDD-99	95.8	97.6	96.2	96.53
Proposed	IBM	NSL-KDD	93.8	96.3	94.6	94.9

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 erred in the classification.

References

[1] S. K. Halgamuge and L. Wang, *Classification and Clustering for Knowledge Discovery*, Springer, Poland, in Studies in Computational Intelligence, vol. 4, pp. 194-209, Discovery, 2005.

[2] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. the Second IEEE Inter-national Conference on Computational Intelligence for Security and Defense Applications*, pp. 53-58, IEEE Press, 2009.

[3] *Estimate motion between images or video frames Block Matching*, The MathWorks, Simulink R2012b, 2012.

[4] S. Mukkamala, "Intrusion detection using neural networks and support vector machine," in *Proc. the 2002 IEEE International Honolulu*, HI, 2002.

[5] M. M. and M. Zulkernine, "A Neural Network Based System for Intrusion Detection and Classification of Attacks," School of computing, Queen University Canada. 2004.
[6] A. Morteza, R. Jalili, and R. S. Hamid, "RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks," *Computers & Security*, vol. 25, no. 6, 459 – 468, 2006.
[7] T. P. Tran, L. Cao, D. Tran, C. D. Nguyen, "Novel intrusion Detection using probabilistic neural network and adaptive boosting," *International Journal of Computer Science and Information Security (IJCSIS)*, pp. 83-91, 2009.
[8] M. Laheeb, "Anomaly Network Intrusion Detection System Based On Distributed Time-Delay Neural Network (DTDNN)," *Journal of Engineering Science and Technology*, vol. 5, no. 4, pp. 457 – 471, 2010.
[9] A. Shahbaa and M. Karma, "Network Intrusion Detection Based On Hybrid Intelligence System," *AL_Rafidain Journal of Computer Sciences and Mathematics*, vol. 9, pp. 81-98. 2012.
[10] L. Vaitsekhovich, "Intrusion Detection in TCP/IP Networks Using Immune Systems Paradigm and Neural Network Detectors," Brest State Technical University, XI International PhD Workshop, OWD 2009.

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.

Dia M. Ali recieved his BSC in Elec. Comm. Eng. From Mosul university in 1992 (Mosul/ Iraq). In 1998 he gets MSC in Elec. Comm. Eng. Mosul University (Mosul / Iraq) and 2007-he recieved a PhD in Comm. Eng. (Network) from Mosul university (Mosul/ Iraq). From 1993 to 2001 he worked at R&D Center Mosul / Iraq. Since 2007 join university of Mosul collage of Engineering as lecture. He interesting in Network Modeling and simulation specially in (OPNET MODELER), Network Security, Mobile Network planning, Antenna modeling and System.