Chapter 7
Hybriding Intelligent Host-Based and Network-Based Stepping Stone Detections

Mohd Nizam Omar and Rahmat Budiarto

Abstract This paper discusses the idea of hybriding intelligent host-based and network-based stepping stone detections (SSD) in order to increase detection accuracy. Experiments to measure the True Positive Rate (TPR) and False Positive Rate (FPR) for both Intelligent-Network SSD (I-NSSD) and Intelligent-Host SSD (I-HSSD) are conducted. In order to overcome the weaknesses observed from each approach, a Hybrid Intelligent SSD (HI-SSD) is proposed. The advantages of applying both approaches are preserved. The experiment results show that HI-SSD not only increases the TPR but at the same time also decreases the FPR. High TPR means that accuracy of the SSD approach increases and this is the main objective of the creation of HI-SSD.

1 Introduction

When the Internet was created, security was not a priority. The TCP/IP protocol security mechanism was thought to be sufficient at the beginning. However, as the Internet usage increases, its security mechanism has become more and more problematic [1]. In fact, as the internet is used widely, the number of attacks also continues to increase. Therefore, attacks or intrusions have always occurred from time to time. There are many techniques that can be used by an attacker or intruder to execute network attacks or network intrusions. A persistent attacker usually employs stepping stones as a way to prevent from being detected [2]. By using Stepping Stone Detection (SSD), the attacker can be detected.

However, due to the complicated patterns of the stepping stones used by the attackers, detection of these stepping stones becomes a challenging task. More

M.N. Omar (✉)
College of Arts and Sciences, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia
e-mail: niezam@uum.edu.my

S.-I. Ao et al. (eds.), *Machine Learning and Systems Engineering*,
Lecture Notes in Electrical Engineering 68,
DOI 10.1007/978-90-481-9419-3_7,

intelligent techniques are required in order to detect accurately the existence of stepping stones by analyzing the traffic pattern from one node to another. Beginning with a research conducted by Standiford-Chen and Herberlein [3] to the latest research by Wu and Huang [4], problems such as accuracy [5] and Active Perturbation Attacks (APA) [6] still remain the top issues among the researchers. An Intelligent-Host-Based SSD (I-HSSD) [7] and an Intelligent Network-based SSD (I-NSSD) [8] have been introduced in our previous research. Nevertheless, they have yet to provide a high rate of accuracy in detecting the stepping stones. We propose a Hybrid Intelligent SSD (HI-SSD) so as to tackle this accuracy problem. The proposed HI-SSD will be compared with other approaches: the I-HSSD and I-NSSD to examine the hybrid approach that has been applied in this research. Experiments will be conducted using a well-planned dataset, and the performance in terms of True Positive Rate (TPR) and False Positive Rate (FPR) [9] will become our main benchmark.

The rest of this article is structured as follows. Section 2 gives research terms used in this research. Section 3 discusses related works and Section 4 describes the proposed approach. In Section 5, we discuss further the experiment and then, a discussion of the results is in Section 6. Finally, we summarize the overall research and present possible future works in Section 7.

2 Research Terms

Before we start in more detail on the experiment, there are several research terms or terminologies used in this work which need to be clarified. In Fig. 1, there are five hosts involved in an SSD environment. Host A is a source of attack and Host E is a victim.

From Fig. 1, Stepping Stones (SS) are hosts A, B, C, D and E. SS = {A, B, C, D, E} where hosts A, B, C, D and E contain the same packet that flows through each host. A Connection Chain (CC), on the other hand, is the connection between hosts A, B, C, D and E. Therefore CC is a, b, c and d. CC = {a, b, c, d}. In Stepping Stone Detection (SSD) research using the Network-based approach (N-SSD), either SS = {A, B, C, D, E} or CC = {a, b, c, d}, can be used to denote the existence of stepping stones.

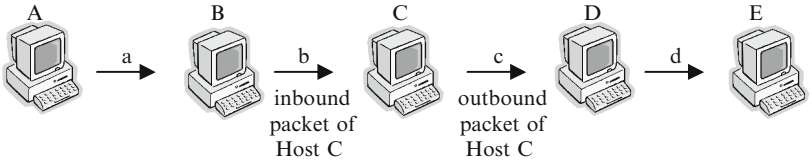

Fig. 1 Detecting a stepping stone chain

Host-based SSD (HSSD), in contrast, works by determining whether or not inbound and outbound connections contain the same packet flow. By referring to Fig. 1, if Host C is referred to, the inbound connection is $CC_c = b$ and the outbound connection is $CC_c = c$. In this case, $CC_2 = CC_3$ or $b = c$.

The challenge to SSD is to find the right solution by determining SS or CC. Overall, SSD research can be divided into statistical- and AI-based SSD, with most of the AI approach comprising the most recent research on SSD. As explained before, SSD research begins with the introduction of statistical-based research such as ON/OFF [10], Thumbprint [3], Deviation [11], and so forth.

3 Related Works

Research by Thames et al. [12] applied the hybrid concept by combining Bayesian Learning Network (BLN) and Self-Organizing Map (SOM) for classifying network-based and host-based data collected within LAN for network security purposes. The experiment was conducted by using four types of analyses (i) BLN with network and host-based data, (ii) BLN with network data, (iii) hybrid BLN-SOM analysis with host and network-based data and (iv) hybrid BLN-SOM analysis with network-based data. The four different types of analyses were required to compare one result to another.

Meanwhile, Bashah et al. [13] proposed a system that combines anomaly, misuse and host-based detection for Intrusion Detection System (IDS). This research only proposed an architecture that combines fuzzy logic and the SOM approach without any implementations/experiments.

Inspired by the above two research works, we hybrid the I-HSSD and I-NSSD approaches and compare the hybrid approach (HI-SSD) with the non-hybrid approaches (I-HSSD and I-NSSD) in terms of accuracy.

4 Proposed Approach: Hybrid Intelligence Stepping Stone Detection (HI-SSD)

The main components of HI-SSD are intelligence and hybrid. The intelligence component comes from the use of the Self-Organization Map (SOM) approach and the hybrid component is created from the combination of Host-based SSD and Network-based SSD. Both components of intelligence and the hybrid are discussed in detail our previous research [7, 8, 14]. Figure 2 shows the HI-SSD architecture.

Figure 2 shows the overall HI-SSD architecture that involves I-HSSD and I-NSSD. In this architecture an intrusion detection system (IDS) is used as a trigger to detect any network intrusion. When an intrusion occurs, I-NSSD starts to capture the network packet in a defined range. At the same time, each host also captures the

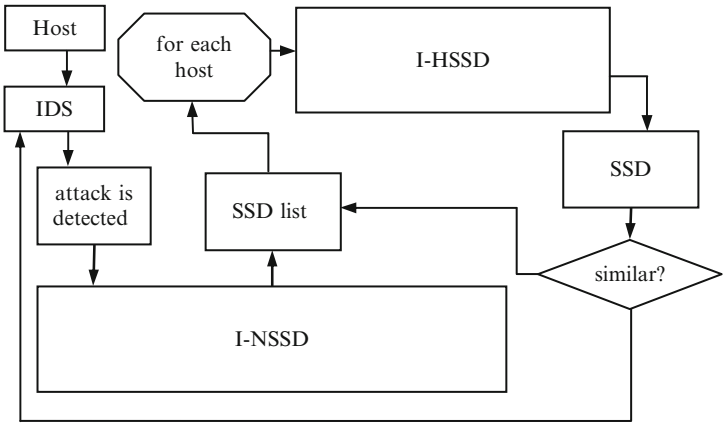

Fig. 2 HI-SSD architecture

network packet as well. When I-NSSD finishes its process to detect stepping stones, information about related hosts involved in the chain of stepping stones is produced. Each host listed in I-NSSD as a stepping stone node then executes a self-examination to check whether it is being used as a stepping stone or not. Results on both I-NSSD's list and I-HSSD's list then are compared. Similarity between these lists shows the real stepping stone host.

For testing purposes, only the functions of HI-SSD, I-NSSD and I-HSSD are involved in the experiment. The development of a fully-functional HI-SSD will become our future work.

The HI-SSD will contain a stepping stone list each from I-NSSD and I-HSSD, while the I-NSSD and I-HSSD will contain a stepping stone list for every network and host respectively. Comparisons will be measured on the TPR and the FPR on each component.

5 Experiment

For the dataset arrangement, Telnet Scripting Tool v.1.0 [15] is used. This is to guarantee a uniform pattern of telnet operations during the execution of the experiment. Here, Telnet represents the interactive connection most frequently used by SSD-related research. Moreover, there is no other dataset that is suitable in this research. Jianhua and Shou-Hsuan [16] used their own dataset. Staniford-Chen and Herberlein [3] also agreed with that.

The experiment is run in a controlled environment so as to avoid any interference with outside networks. Wireshark [17], on the other hand, is used to capture network packets that flow in each host. After the Telnet Scripting tool has ended its run, information pertaining to the packets is converted into text-based form. This is

done in order to proceed to the consequent processes to acquire the appropriate information needed later. In this research, only time information is needed. This time information from the experiment is transferred into m-type file to be used later with Matlab 6.1 [18] software. In Matlab 6.1, the time information is used as the input to create, train, and lastly, to plot the SOM graph. The result from the visualization is taken as the result of this research and will be discussed in the next section.

Although the result for HI-SSD is obtained from I-NSSD and I-HSSD, this work will show the benefit of stepping stone detection when information obtained from a combination of the two approaches is compared to two separate sets of information when using I-NSSD or I-HSSD alone.

Figure 3 shows the layout of the overall experiment. From the figure, it explicitly shows that four hosts are involved in the stepping stone.

From these four stepping stone hosts, there are three connection chains (C_1, C_2, and C_3) involved. That means that only four stepping stones or three connections should be detected by the SSD approach. Increased number of detections causes lower TPR and decreased number of detections causes higher FPR. Table 1 shows the relationships for each host and its connection chains.

Based on the location of each host in Fig. 1, Table 1 shows the number of possible connection chains for each host and its list. The number of connection chains has been made based on the assumption that Host 1 and Host 4 are the starting and ending points respectively. Host 2 and Host 3 contain two different types of connection chains, one and two. However, connection chains that contain

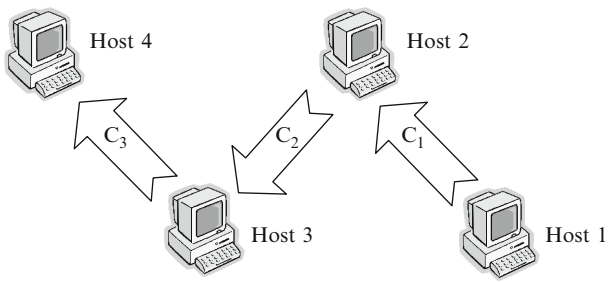

Fig. 3 Experiment layout

Table 1 Host and its relationship

Host	No. of connection chain	Connection chain list
Host 1	3	c_1, c_2, c_3
Host 2	1	c_1
	2	c_2, c_3
Host 3	2	c_1, c_2
	1	c_3
Host 4	3	c_1, c_2, c_3

just one connection can be eliminated because one connection does not mean that it is a stepping stone connection. In fact, research by RTT-based SSD [19–21] agreed that only connection chains with more than three connections can be considered as stepping stone connections. Based on our previous research [8], the existence of two connections onwards is enough for a chain to be identified as a possible stepping stone chain.

To calculate the effectiveness of the tested approach, TPR and FPR are used.

$$\text{FPR} = \frac{\text{number of false positive}}{\text{number of possible negative instances}} \tag{1}$$

False Positive Rate (FPR) refers to the fraction of negative instances that are falsely reported by the algorithm as being positive. In this situation, the algorithm has detected the connection chains which exist even though it is not true.

$$\text{TPR} = \frac{\text{number of true positive}}{\text{number of possible true instances}} \tag{2}$$

True Positive Rate (TPR) refers to the fraction of true instances detected by the algorithm versus all possible true instances. The discussion on the result and its analysis will be presented.

6 Result and Analysis

Result on each type of SSD will be discussed in each of the following sub-section. As described before, we have chosen to use SOM as the intelligent approach. As a result, the SOM graph will represent each compared solution.

6.1 Intelligence Network Stepping Stone Detection (I-NSSD)

In I-NSSD, the results are obtained from the execution of SOM approach through the arrival time for the overall captured data in the network. In this case, only one graph has been produced. It is different from I-HSSD that needs one graph for each host involved. Figure 4 shows the result.

In contrast to the I-HSSD approach that depends on the number of possible straight lines which can be created to determine the number of connection chains, the I-NSSD approach is based on the number of possible groups generated. In Fig. 4, four possible groups of SOM nodes can be counted (labeled as a, b, c and d). Thus, there are four connection chains involved in the experiment. However, the true number of connection chains involved in this research is only three. Therefore,

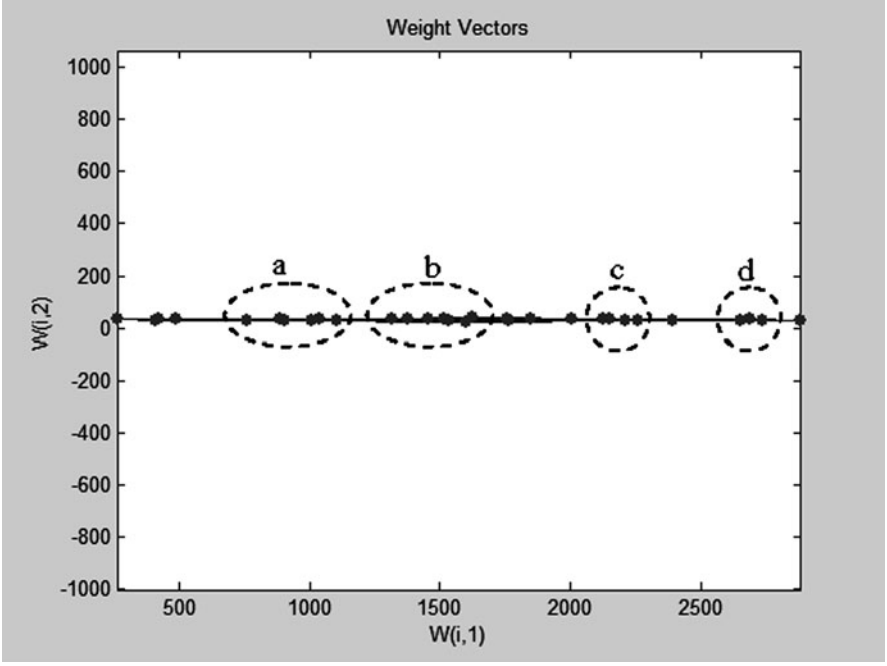

Fig. 4 Node of SOM in I-NSSD

there exist false positive reports in the I-HSSD experiment. By using formula (1), FPR for I-NSSD is 33.3%. For TPR, I-NSSD shows 100% achievement.

6.2 Intelligence Host-Based Stepping Stone Detection (I-HSSD)

As described previously, I-HSSD involves every host that has been listed in I-NSSD. In this case, arrival time for each host is run by using the SOM approach. Each result is an output from the execution.

Figure 5 shows that three possible directions can be traced (e, f and g). That means there are three possible connections which exist in the originating host, Host 1. Based on the value from Table 1, Host 1 obtains 100% TPR and 0% FPR.

Figure 6 on the other hand shows that there are two connection chains (h and i) that could possibly exist in Host 2 as the monitored host. Based on the number of connection chains from Table 1, Host 2 got 100% TPR and 0% FPR.

In Fig. 7, similar to Fig. 6, there are two connection chains (j and k) that could possibly exist in this graph. Based on the number of connection chains from Table 1, Host 3 also got 100% TPR and 0% FPR.

Figure 8 shows the last node of SOM that needs to be observed. From the graph, there are two possible obtainable directions. That means that two connection chains

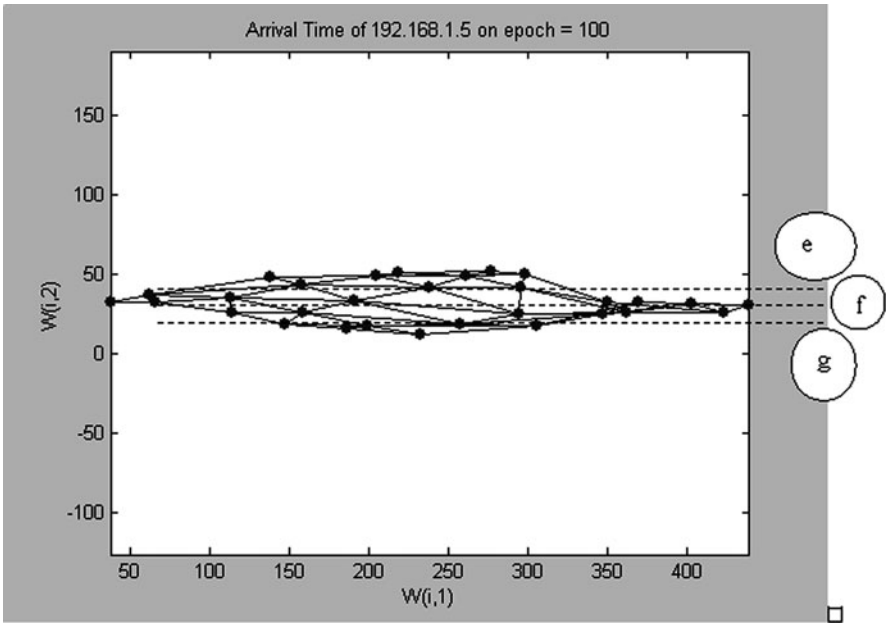

Fig. 5 Node of SOM on Host 1

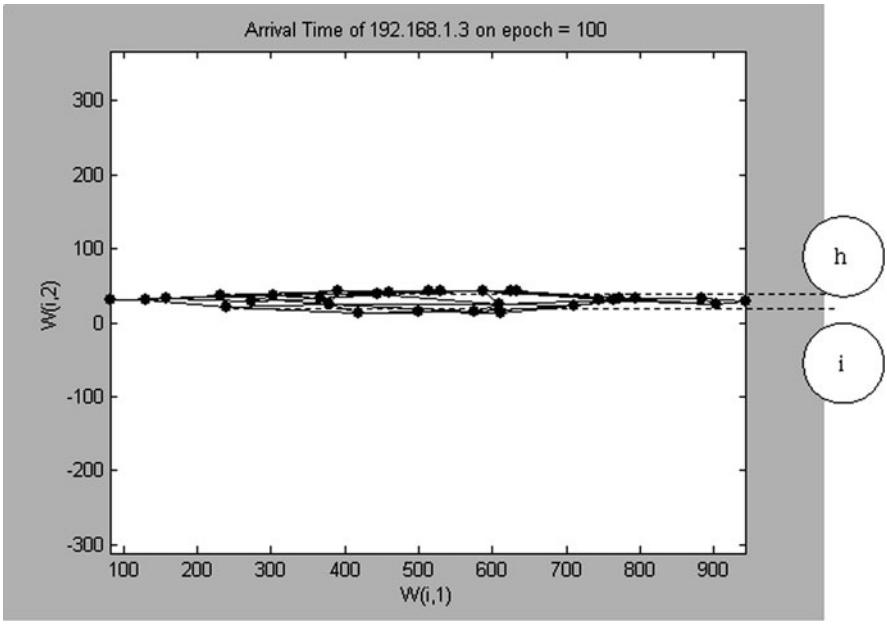

Fig. 6 Node of SOM on Host 2

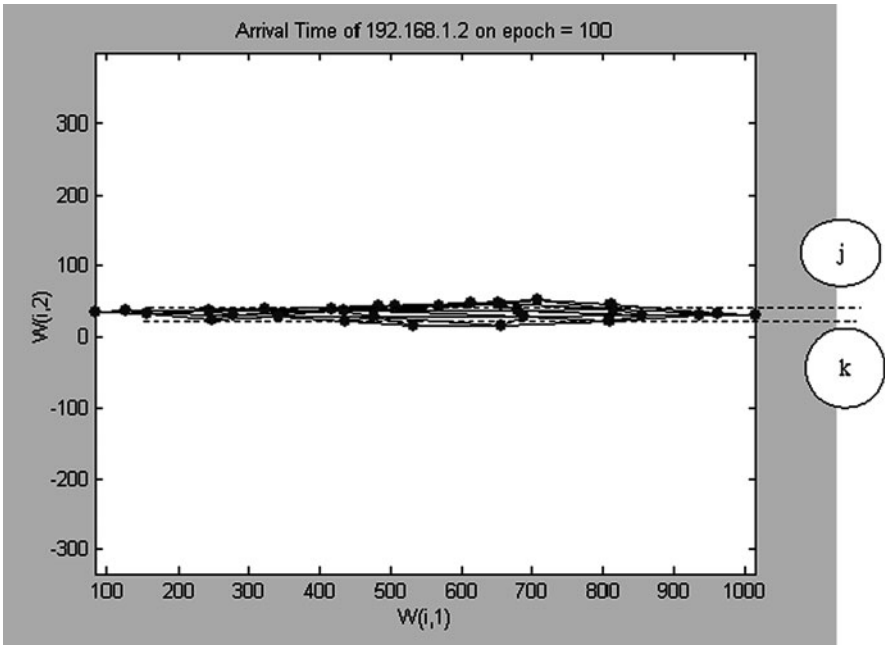

Fig. 7 Node of SOM on Host 3

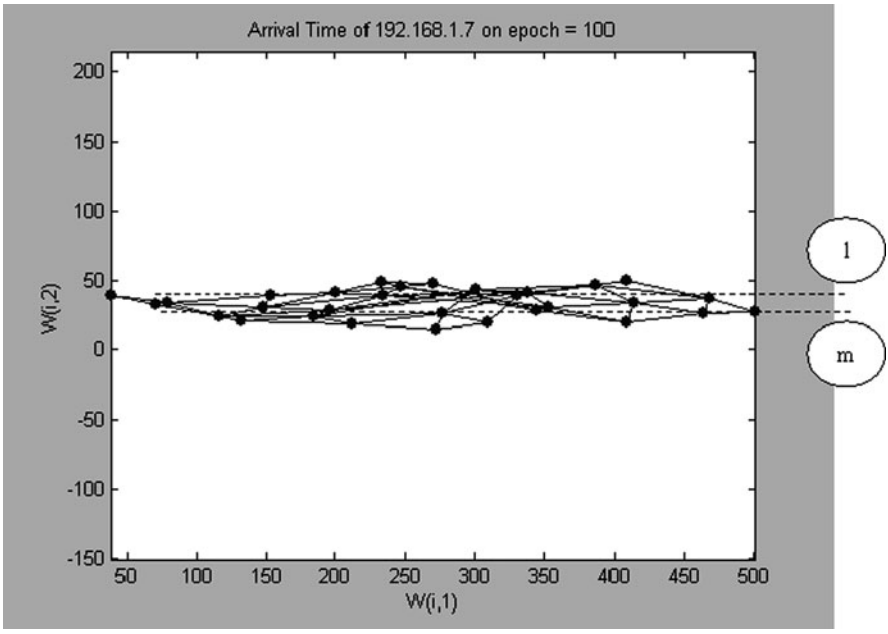

Fig. 8 Node of SOM on Host 4

Table 2 I-HSSD experiment result

Host	No. of connection chain	No. of connection chain detected	TPR (%)	FPR (%)
1	3	3	100	0
2	2	2	100	0
3	2	2	100	0
4	3	2	66.7	0

(l and m) have been detected. However, based on the number of connection chains in Table 1, three connection chains should have been detected in Host 4. For that reason, I-HSSD in Host 4 miss-detects another connection. In this case, the TPR becomes 66.7%. The FPR on the other hand also gives 0%.

From the result on each host, it shows that only the result of Host 4 does not achieve 100% TPR. This can be considered as a weakness of the I-HSSD. Table 2 shows the result of the I-HSSD experiment.

Based on the overall result of the I-HSSD experiment, connection chains have been successfully detected in Host 1, Host 2 and Host 3. In Host 4, although the connection chains have also been successfully detected, the number of connection chains detected is less than the actual number involved. This makes the TPR at just 66.7%. On the other hand, the FPR is the same for all hosts.

6.3 Hybrid Intelligence Stepping Stone Detection (HI-SSD)

As described earlier, HI-SSD is constructed from the combination of I-HSSD and I-NSSD. Therefore, the information from I-HSSD and I-NSSD is still used in the HI-SSD. As shown in Fig. 2, the information obtained from I-HSSD and I-NSSD are rearranged so as to generate a more accurate stepping stone detection result compared to the use of I-HSSD or I-NSSD alone.

For this purpose, the first information acquired from I-NSSD is observed. From the result, four connection chains are detected. At this level, false detection still not has been discovered. All information needed is distributed to the related hosts. The host which is related to the list then runs the I-HSSD function by itself. This is to check whether or not the host is used as a stepping stone. In this case, Host 1, Host 2, and Host 3 have successfully detected the number of existing connection chains. However, Host 4 has just detected two connection chains compared to three connection chains that should have been detected.

Although miss-detection has occurred here, the number of maximum possible hosts from Host 1 helps a lot to balance the Host 4 result. From the I-HSSD result, it is shown that there are only three connection chains involved compared to four proposed by I-NSSD. Combining I-HSSD and I-NSSD avoids false and miss-detections. By using both I-HSSD and I-NSSD, it is shown that 100% TPR and

Table 3 Experiment result

Type of stepping stone detection approach	TPR (%)	FPR (%)
I-NSSD	100	33.3
I-HSSD	91.67	0
HI-SSD	100	0

0% FPR has been achieved. For a clear picture on the overall HI-SSD, the related algorithm is given as follows.

Begin
I-NSSD:
capture network packet
collect arrival time
execute SOM
count the group of node, n
list involved host, l
sent n & l to I-HSSD
I-HSSD:
activate I-HSSD on selected host based on l
for 1 to n
execute SOM
count the possible straight line,
identify the existence of connection chain for the host, e
end for
End

Result of the experiment according to the percentage of TPR and FPR obtained from I-NSSD, I-HSSD and HI-SSD respectively is tabulated in Table 3.

Table 3 shows the experiment result of I-NSSD, I-HSSD and HI-SSD. As described previously, HI-SSD is a combination of I-NSSD and I-HSSD. Therefore, the TPR and FPR for HI-SSD is the combination of I-NSSD's TPR and FPR and I-HSSD's TPR and FPR. In the other words, the average TPR and FPR of I-NSSD and I-HSSD become the result of HI-SSD. In this case, 100% TPR and 0% FPR for HI-SSD is better than the use of I-NSSD or I-HSSD alone. Although I-NSSD shows 100% TPR, but the 33.3% FPR can adversely affect the overall function of stepping stone detection. In the I-HSSD, 100% FPR makes this approach free of false detection. However, 91.67% TPR is not enough to render this approach to be fully-functional. As a result, combining both I-NSSD and I-HSSD to form the HI-SSD will balance the TPR and the FPR at the same time.

7 Conclusion and Future Work

The goal of this research is to prove the effectiveness of the proposed HI-SSD which is actually a hybrid or combination of I-NSSD and I-HSSD. From the experiment, it is shown that the HI-SSD is more accurate compared to both

I-NSSD and I-HSSD. Therefore, it is proven that HI-SSD is more accurate compared to I-NSSD or I-HSSD.

In the future, we will improve our approach to be more robust towards active perturbation attacks such as delay, packet drop and chaffing. Testing on the active perturbation problem would not only be executed onto our proposed solution, but it would also involve our closest research that used the Data Mining approach. By doing this, we not only can measure the proposed approach's capabilities but at the same time can also compare it with other similar approaches.

Only one dataset is used in this experiment. With the intention of verifying the capability of the proposed HI-SSD, we need different types of dataset. Our observation on the datasets used in SSD-based research has shown that there are two kinds of datasets which can be used; datasets generated by ourselves and public datasets. By using various kinds of datasets instead of just one type of dataset, the true capabilities of the approach can be examined more. As such, testing the proposed HI-SSD on top of different datasets is one of our future works.

Another future plan is to compare the proposed HI-SSD approach with the statistical-based approaches. Therefore, to ascertain that the proposed approach is better than statistical-based approaches, it is good to involve the different approaches together in the experiment.

Lastly, for a true experience of a fully-functional stepping stone detection, the overall approach should be translated into a full system. If a complete system is created, comparisons with other approaches could be made more easily.

References

1. C. Chamber, J. Dolske, J. Iyer, *"TCP/IP Security" , Department of Computer and Information Science* (Ohio State University, Ohio 43210). Available at: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html
2. K.D. Mitnick, W.L. Simon, The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers" (Wiley, 10475 Crosspoint Boulevard, Indianapolis, IN 46256, 2005)
3. S. Staniford-Chen, L.T. Herberlein, Holding intruders accountable on the Internet, in *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, Oakland, CA, 1995, pp. 39–49
4. H. Wu, S.S. Huang, Neural network-based detection of stepping-stone intrusion. Exp. Sys. Appl. **37**(2), 1431–1437 (March 2010)
5. A. Blum, D. Song, S. Benkataraman, *Detection of Interactive Stepping Stone: Algorithm0020and Confidence Bounds*, vol 3224/2004. Lecture Notes in Computer Science (Springer Berlin/Heidelberg, 1 Oct 2004), pp. 258–277
6. X. Wang, *Tracing Intruder BStepping Stone*. Ph.D. Thesis, North Carolina State University, Raleigh, 2004.
7. M.N. Omar, R. Budiarto, Intelligent host-based stepping stone detection approach, in *Proceeding of The World Congress on Engineering and Computer Science 2009*, vol II, San Francisco, USA, 20–22 Oct 2009, pp. 815–820
8. M.N. Omar, R. Budiarto, Intelligent network-based stepping stone detection approach. Int. J. Appl. Sci. Eng. Technol. **53–135**, 834–841 (2009)
9. A. Almulhem, I. Traore, Detecting connection-chains: a data mining approach. Int. J. Netw. Security. **11**(1), 62–74 (Jan 2010)

10. Y. Zhang, V. Paxson, Detecting stepping stones, in *Proceedings of the 9th USENIX Security Symposium*, Denver, CO, 2000, pp. 67–81.
11. K. Yoda, H. Etoh, Finding connection chain for tracing intruders, in *Proceedings of the 6th European Symposium on Research in Computer Security (LNCS 1985)*, Toulouse, France, 2000, pp. 31–42
12. J.L. Themes, R. Abler, A. Saad, Hybrid intelligent system for network security. ACM southeast regional conference 2006, 2006.
13. N. Bashah, I.B. Shanmugam, A.M. Ahmed, Hybrid intelligent intrusion detection system, Proc. World Acad. Sci. Eng. Technol. **6** (2005)
14. M.N. Omar, L. Serigar, R. Budiarto, Hybrid stepping stone detection method. in *Proceeding of 1st International Conference on Distrubuted Framework and Application (DFmA 2008)*, Universiti Sains Malaysia, Penang, 21–22 Oct 2008, pp. 134–138
15. Wareseeker (2008) [Online] Available: http://wareseeker.com/freeware/telnet-scripting-tool-1.0/19344/TST10.zip 8 Feb 2008
16. Y. Jianhua, S.H. Shou-Hsuan, A real-time algorithm to detect long connection chains of interactive terminal session", in *Proceedings of the 3rd International Conference on Information Security*, China, 2004, pp. 198–203
17. Wireshark (2009). [Online] Available: http://www.wireshark.org 8 Feb 2009
18. H. Duane, L. Bruce, *Mastering MATLAB A Comprehensive Tutorial and Reference* (Prentice-Hall, New Jersey, 1996)
19. K.H. Yung, Detecting long connection chains of interactive terminal sessions, in *Proceedings of the International Symposium on Recent Advance in Intrusion Detection (RAID 2002)*, Zurich, Switzerland, 2002, pp. 1–16
20. J. Yang, S.S. Huang, A real-time algorithm to detect long connection chains of interactive terminal sessions, in *Proceedings of the 3rd International Conference on Information Security (INFOSECU 2004)*, Shanghai, China, 2004, pp. 198–203.
21. J. Yang, S.S. Huang, Matching TCP packets and its application to the detection of long connection chains on the internet, in *Proceedings of the 19th International Conference on Advance Information Networking and Applications (AINA 2005)*, Tamkang University, Taiwan, 2005, pp. 1005–1010