Acta Scientific COMPUTER SCIENCES

Volume 4 Issue 1 January 2022

Review Article

A Review of Recent Progress in Stepping-stone Intrusion Detection

Lixin Wang* and Jianhua Yang

TSYS School of Computer Science, Columbus State University, Columbus, Georgia, USA

***Corresponding Author:** Lixin Wang, TSYS School of Computer Science, Columbus State University, Columbus, Georgia, USA.

Received: December 03, 2021

Published: December 23, 2021

Abstract

Hackers on the Internet usually send attacking commands through compromised hosts, referred to as stepping-stones, in order to avoid being detected. Stepping-stone intrusion (SSI) is a hacking technique used by intruders to launch cyber-attacks and allows them to hide behind a long connection chain. In an SSI attack, an intruder employs a chain of stepping-stones as relay hosts and remotely connect these stepping-stones using software like SSH.Due to the nature of the TCP protocol, an interactive session of a TCP connection between a client and a server is independent of other sessions in the connection. Therefore, it is extremely hard to detect the origin of the attack if an intruder gained unauthorized access to a remote target system through multiple relayed TCP sessions. The final target of a TCP connection chain may only capture the traffic from the last session of the chain, but can hardly learn any information about the attacker machine. There are quite a few recent significant and innovative approaches for SSI detection (SSID) that have not yet been reviewed and compared with other similar SSID approaches. This paper conducts a research survey on most of the significant approaches proposed for SSID by far with the inclusion of all recent progress in this area. The SSID methods reviewed in this paper are categorized into two different types: host-based and network-based approaches, according to the number of the hosts that play a key role in the SSID algorithmdesign. The contributions and limitations of every SSID approach included in this paper are clearly described and compared with similar SSID approaches proposed in the literature.

Keywords: Stepping-stone Intrusion; Intrusion Detection; Network Security; Connection Chain; Interactive Session

Abbreviations

SSI: Stepping-stone Intrusion; SSID: Stepping-stone Intrusion Detection

Introduction

Hackers on the Internet usually send attacking commands through compromised hosts, referred to as stepping-stones, in order to avoid being detected. SSID has been attracting much attention of network security researchers since the seminar work [1] by Staniford-Chen., *et al*. which proposed a "content-thumbprint" method for SSI published in 1995. A great number of approaches for SSID have been proposed since then. There are quite a few recent significant and innovative detection approaches for SSI that have not yet been reviewed and discussed. This paper conducts a research survey of recent progress in stepping-stone intrusion detection. These detection methods for SSI proposed in recent years are categorized into two different types: host-based and network-based approaches, based on the numberof the hosts that play a key role in the design of the SSI detection algorithms. In this section, we briefly introduce somebasic concepts including SSI, SSID, host-based SSID, and network-based SSID.

Stepping-stone intrusion

Accessing a server remotely have lots of benefits and it is much more convenient for its users. Howerver, allowing remote access makes the servers in the risk of possible unauthorized access. Those malicious users who illegally gained unauthorized access to a remote server are referred to as intruders, or hackers. Hackers can either directly or indirectly access a server to obtain sensitive information, money, or critical military information. However, directly accessing a remote server might quickly be caught as the source IP of every packet can be easily obtained in the captured packets using software tools such as Wireshark,TCPDump, or some other similar tools.

Hackers tend to gain access to a remote server indirectly, in order to minimize the chance of being detected and caught. Due to the nature of the TCP protocol, an interactive session of a TCP connection chain between a client and a server is independent of other sessions in the chain. Therefore, it is extremely hard to detect the origin of the attackerif he/she gained unauthorized access to a remote target system through multiple relayed TCP sessions. The final targetof a TCP connection chain may only capture the traffic from the last session of the chain, and it can hardly learn any information about the attacker machine. Most attacks using stepping-stones are hard to be traced back for political and geographical reasons. If an SSI via stepping-stones could be detected within the period of attacking, then the session can be cut off and the target host can be protected. Even though there are still a few researchers working on the traceback of stepping-stone intrusion, most network security researchers have been working on stepping-stone intrusion detection by far.

Stepping-stone intrusion detection

In order to conduct SSID, it is required to create a connection chain as shown in figure 1 using a remote-login program such as SSH to send the attacking command. In figure 1, Host 0 is assumed to be used as the attacker machineto launch a cyber attack to the target system Host N through the stepping-stones: Host 1, Host 2, …, Host k-1, Host k,Host k+1, …and Host N-1 that are the intermediate hosts. SSID can be conducted on any one of the stepping-stones. In figure 1, we assume Host k has a detection program installed and is referred as a detecting sensor or a sensor. SSIDis to determine if the sensor Host k is used as a stepping-stone for intrusion. An incoming connection of Host k is defined as the connection from Host k-1 to Host k, and an outgoing connection of Host k is any connection from Hostk to Host k+1. If there exists one relayed connection pair between all the incoming connections and all the outgoing connections of Host k, then Host k is used as a stepping-stone.

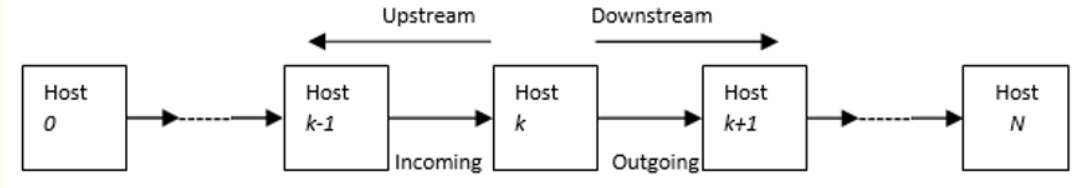

Figure 1: A Sample Connection Chain.

A basic method for SSI is to compare all the outgoing connections of a detection sensor with its all the incomingconnections to see if there is a relayed connection pair. This type of approaches is referred to as the host-based SSID and will be discussed in Section 2. It is easy to see that this type of detection approaches for SSI could produce high false-positive errors due to the legal use of stepping-stones by some applications for accessing remote servers.

In order to bring down the false-positive errors incurred with the host-based SSID, another type of approaches for SSID was developped by estimating the length of a connection chain, which is the number of connections from theattacker host to the final target host in the chain. This type of detection methods is referred to as network-based SSID.If the length of a connection chain is at least three, it means that a user attempts to gain access to a target

host through three or more machines. It is a common sense that the more machines are employed in a connection chain to access a remote server, the slower the network communication. If there are no malicious activities involved, it does not makeany sense to login to a remote server through three or more machines. Three is a threshold number used by most researchers because it was investigated and verified that most legal applications fairly employ three or more other machines on the Internet to gain access to a remote server.

The part of the connection chain from Host 0 (the attacker host) to Host k (the sensor host) as shown in figure 1 is referred to as the upstream connection, and the part of the connection chain from Host k (sensor host) to the targetHost N is referred to as the downstream connection. Unfortunately, to the best of our knowledge, it is extremely difficult to estimate the length of a upstream connection. Thus, it is difficult to estimate the length of a whole connection chain. However, knowing the length of a whole connection is the only way to avoid false-negative error inSSID. In the literature of SSID, most network security researchers have been using the length of a downstream connection to decide where there is an SSI. Therefore, network-based SSID methods could generate false-negative errors.

Host-based SSID

If a machine is used as a stepping-stone host, it should have a relayed pair of connections between its incoming and outgoing ones. SSID is to decide if a host is used as a stepping-stone for intrusion. For host-based SSID, the incoming and outgoing connections of a host are compared to see if there is a relayed pair of connections. To determineif a host is used as a stepping-stone, all the outgoing and incoming connections of a host must be examined. If there exists such a pair of connections, it is highly possible that the host is used as a stepping-stone for intrusion by attackers. In this section, we conduct surveys for existing significant host-based approaches for SSID proposed in the literature,including some recent detection methods proposed for SSI.

A lot of host-based detection approaches have been proposed to examine if a host is used as a stepping-stone sincethe seminar work [1] by Staniford-Chen., *et al*. published in 1995. This paper proposed a "content-thumbprint" methodfor SSI by comparing the content of the packets from an incoming connection with an outgoing one of a host. If the content matches, then they are a relayed pair of connections. However, this "content-thumbprint" method for SSI only works when the network traffic is not encrypted. Thus, this method does not work when the network traffic is encrypted.

To overcome the shortcoming of the "content-thumbprint" approach proposed in [1], a "time-thumbprint" method was proposed in another seminar work [2] by Zhang., *et al*. This method makes the decision for whether thereis a matched pair of connections by analyzing the timestamps of packets. Since packets' timestamps are not encryptedduring data communication, this "time-thumbprint" method works well for SSID when the network traffic is encrypted. However, this approach of using "time-thumbprint" does not work effectively if the sessions are manipulated by intruders using evasion techniques such as chaff-perturbation or time-jittering.

K. Yoda., *et al*. [3] proposed a deviation-based detection approach by setting up monitors for packets at many nodes on the Internet to store attackers' activities. This method is similar to the one proposed in [2]. Yoda's method in [3] used the deviation between two sessions. If a machine is employed as a stepping-stone to gain access to a remotetarget system, the packets information at the hosts we recorded are compared to find the closest match. The deviation for one packet stream on a connection from another is defined and computed. If such a deviation is small, the two connections should belong to the same chain. The less the deviation, the larger the chance for the two sessions to be relayed. This approach attempts to find a set of data streams that might match the one directly sent from the originalattacker's machine.

[2,3] have some common issues when the network traffic are manipulated by intruders using evasion techniques such as either chaff perturbation or time-jittering, both the time-based method and the deviation-based approach for SSID in [2,3], respectively, are significantly affected. The intruder's active timing perturbation andinjection of meaningless chaff packets by the attacker make the SSID process more difficult. Since then several SSID approach were developed to g*et al*ong these issues.

[4] by D. Donoho., *et al*. proposed a method for SSID by monitoring the outgoing and incoming network traffic of a gateway router. This paper used a different approach by considering a gateway router as a stepping-stone. A pairof outgoing and incoming connections of a gateway router is referred to as a stepping-stone pair of

connections if those connections are used for a stepping-stone intrusion. The detection method developed in [4] is in the category of a host-based approach. That is, the incoming and outgoing connections of a gateway router are compared to see if there is a relayed pair of connections. An advantage of this method is that the network traffic can be encrypted as wellas it is theoretically resistant to intruders' session manipulation to a certain degree.

[4] by A. Blum., *et al*. proposed a Detect-Attacks-Chaff stepping-stone detection algorithm (DAC) for SSID by counting the number of packets of a connection. This paper [5] employed the ideas from Computational Learning Theory and conducted analysis using the concept of random walks. Blum's method for SSID used the idea that two sessions are relayed if and only if the difference between the packet numbers in the two sessions is bounded above. This method was known to be a good SSID approach that could be resistant to intruders' evasion manipulation usingthe time-jittering technique, but Blum's method does not work effectively in resisting to intruders' evasion manipulation with chaff-perturbation as the upper bound for the number of monitored packets may be huge.

The work [6] by T. He., *et al*. proposed the packet counting detection algorithms aiming to handle the issues caused by intruders' session manipulation. First the authors considered detecting stepping-stone pairs with bounded perturbation without chaff packets injected, and then they generalized their detection approach to handle network traffic with injected chaff packets. This paper proposed two activity-based algorithms for SSID. The key ideaused in this work is defining a stream pair to be normal if the optimal inserting algorithm could have had to insert a certain fraction of meaningless chaff packets to let the attacking packets be embedded into the given stream pair. These detection algorithms developed in [6] for SSID worked well when the network packets suffered jittered-timingas well as a small amount of chaffed meaningless packets into an attacking data stream. However, the two detection algorithms using packet counting proposed in [6] only work effectively at a low packet-chaff rate.

Another detection method by J. Yang., *et al*. in [7] was developed by using random-walk to resist attackers' sessionmanipulation with chaffed meaningless packets. [7] modeled the differences between the number of responses and the number of requests as a random-walk process. It was verified by the authors in [7] that if the two connections area matched pair, then the behavior of the above difference is a random-walk process.

The paper [8] by J. Yang., *et al*. improved the ideas in [7] and proposed an RTT-based random-walk detection method for SSI, in which whether an outgoing connection and an incoming one are a matched pair is determined by applying the number of RTTs in a connection as well as the modelling of using random-walk method. Experiment results obtained in [8] showed that the RTT-based random-walk approach can defeat intruders' session manipulation more effectively than the one proposed in [7] by using the number of monitored packets, with either jittered-timing or chaff perturbation evasion technique.

A software to inject chaff-packets into an interactive TCP connection was developed in [9] by Yang., *et al*. in 2018.This software can be easily used to determine whether or not a proposed SSID method can work effectively to resist session manipulations with chaff-perturbation by attackers. A framework to test whether a detection algorithm for SSI is resistant on time-jittering evasion was developed in [10] by L. Wang., *et al*. Network security researchers can usethe software tool developed in [9] or the framework proposed in [10] to conduct network experiments by manipulatinga TCP connection with either chaff-perturbation or time-jittering evasion technique, and determine whether their proposed approaches for SSID are resistant on session manipulations by intruders.

[11] by Y. Zhang., *et al*. developed a SSID method using context-based packet matching aiming to resist session manipulation by intruders. The simulation results obtained in this paper verified that if attackers send attacking packets to a network with chaff-rate 100%, this SSID method proposed in [11] is still able to match the outgoing and incoming connections for SSID as well as works effectively in resisting chaff-perturbation by intruders.

Timing-based correlation SSID methods are subject to time-jittering session manipulation by intruders. [12] developed a watermark-based-correlation approach for SSID that worked well when the network traffic is manipulated by intruders with time-jittering evasion technique. This watermark-based approach embeds a special watermark into the network traffic that is encrypted with the jitted time-stamps of the packets that were selected by the algorithm. This method based on a special embedded watermark has

several superiorities over those existing timing-based correlation SSID methods in resisting timing perturbations by the attacker, as this watermark-based correlation proposed in [12] does not need any assumptions for the distribution of the time-stamp differences of the captured TCP packets.

M. Gamarra., *et al*. [13] constructed a graph according to vulnerabilities of Internet of Things (IoT) systems and then developed a framework of characterizing stepping-stone intrusions in the IoT systems based on the vulnerabilitygraph. A linear system is used to formulate the dynamics of stepping-stone hosts in the IoT systems. The frameworkproposed in this paper is also extended to a real-world situation when the graph of vulnerabilities changes after the intrusion to the IoT systems has been found by existing intrusion detection system on the IoT. However, network traffic with session manipulation by intruders were not taken into consideration in this paper.

[14] by J. Yang., *et al*. developed a new approach for SSID that can effectively resist session manipulation by intruders using ideas of packet cross-matching as well as the concept of random walks. Prior approaches proposed for SSID can only work effectively in resisting session manipulation by intruders with limited capabilities. The technical analysis conducted in this paper showed that SSID approach proposed in [14] may effectively defeatintruders' session manipulation using chaff-perturbation evasion technique with unlimited number injected packets.A recent work [15] by H. Clausen., *et al*. proposed a framework to simulate stepping-stone behaviros in a realistic scenario by using effective evasion tools such as time-jittering and/or chaff-perturbation to release a large dataset. Thedatasets are analyzed to produce the effective rates for SSID of eight selected known state-of-the-art detectionalgorithms in the literature. The framework proposed in this paper may help network security experts to create a model to characterize the SSI behaviors.

However, it is well-known that some legal applications might access a remote server by employing stepping-stonehosts. Therefore, host-based SSID approaches could generate false-positive errors. More specifically, if an application uses a stepping-stone to access a server remotely, we cannot say that the remote access must be a malicious intrusion.A typical example for this is described as follows: In order to access a remote web server through a client web browser,this process may involve accessing a database server that is running on a separate remote server. Based on the scenariowe describe here, from the user browser to the remote web server, finally to the remote database server, the web serverin such a case serves legally as a stepping-stone host.

Network-based SSID

To get around the disadvantages of host-based SSID approaches, some other detection methods for SSI by estimating the length of a connection chain were developed as described in the literature, referred to as network-basedSSID. The longer a connection chain is, the higher the probability that the chain is used for malicious intrusion. Due to the challenges of estimating the length of the upstream section in a connection chain, most network-based SSID algorithms proposed by far focused on estimating the length of the downstream section in a connection chain, instead of the whole connection chain. Therefore, host-based SSID approaches using the length of a connection chain could generate false-negative errors.

Using a stepping-stone to access a remote server is common in legitimate applications, but it is very rare that threeor more stepping-stones are employed to access a remote server. Clearly, the more machines are used to access a remote server, the slower the network communication. It won't be necessary to access a remote server through three or more stepping-stones as this accessing process could produce too much traffic and make it very ineffective. Therefore, it is assumed that legal applications use at most two intermediate stepping-stone hosts to access a remote server.

There are many approaches that have been developed through estimating the length of a connection chain for SSID. [16] by K. Yung., *et al*. developed the first detection method for SSI by employing the length of a connection chain. Their main idea for estimating the connection chain length is to match a Send packet with an acknowledgement packet sent directly from the adjacent host in the connection chain. In [16], the way to match a Send with an Echo doesnot work well. In some cases, it may even incur an error for matching TCP packets. As a result, it is impossible to estimate the length of a connection chain accurately. Yard-stick effect is another severe issue existing in K. Yung's approach. That is, using the length of a connection from a sensor to its adjacent connected host as the yard to measurethe length of the downstream connection chain may not be appropriate in some extrema cases. For example, a too long or too short yard may make the same connection chain

shorter or longer than it actually is. All of these happen due to incorrect packet matching algorithm used in [16]. Consequently, the network-based SSID method proposed in [16] produced high false-negative error as well as high false-positive error. Therefore, this method cannot be considered as an effective one for SSID.

[16] by Yang., *et al*. proposed a better approach referred to as the step-function detection method to estimate the length of a connection chain than the method proposed by K. Yung in [16]. In the setting of a local area network, the step-function SSID approach proposed in [17] produced much less false-positive error as well as false-negative errors. Compared to the Yung's approach proposed in [16], this step-function method used a totally different way to match TCP pakcets so thatthe length of a connection chain from the sensor host to the victim can be estimated correctly. The network experiment proposed in [17] began with a chain of only one connection. Gradually, the length of the connection chain is extended to two, three, four and five, respectively. Eventually, a connection chain of length five was set up. In this way, the step-function SSID approach can match a Send packet with its corresponding Echo packetsent from the target host. A drawback of this step-function method is that it only works well in the setting of a LAN environment. This method does not work well and cannot be used in the context of the Internet as the rate of packet-matching is very low.

The SSID algorithm proposed in [18] is to overcome the limitation suffered from the step-function method proposed in [17] and applied a data clustering and partitioning method to match a Send packet with its corresponding Echo packet and to find the RTTs of the packets captured from a connection chain. Previous network-based methods of matching Send and Echo packets only worked well locally. The data mining algorithm proposed in [18] employed a global approach for packet matching. It checks all the captured packets and then determines a match of a Send packet and its corresponding Echo packet. More specifically, this method captured all the Send and Echo packets of a connection chain in a certain time interval and calculated the time differences between each Send packet and all the Echo packets received after it. Therefore, the correct RTTs must a subset of the calculated time differences. Based on this observation, the approach is to find the subset that truly represents the round-trip times. This method can achievehigh rates of packet matching as it matches the Send and Echo packets in a global scene than the all previously proposed algorithms for SSID. As a result, the data clustering and partitioning method for SSID proposed in [18] notonly achieved high packet matching rates, but also produced both low false-negative error and low false-positive error in terms of detecting stepping-stone intrusion.

However, the SSID method proposed in [18] requires capturing and processing a large amount of TCP packets and mines network traffic in an inefficient way, and thus the method is not efficient in term of the computation time used to process the captured packets. If the dataset size is doubled, then the running time of SSID detection approach proposed in [18] will increase four times. The SSID method proposed in [19] by L. Wang., *et al*. is one of the methods developed to overcome this drawback of data clustering and partitioning method proposed in [18]. [19] proposed a new SSID approach by mining network traffic using the k-Means clustering method to estimate the length of a connection chain. This SSID method is simpler and runs more efficient as it does not require that a large number of packets must be captured. Also, this k-Means clustering based SSID algorithm can resist session manipulation by intruders with chaff-perturbation to a certain degree. However, this SSID approach based on k-Means clustering doesnot work effectively if there are many RTT outliers of the captured TCP packets in the Internet environment. [20] by Y. Sheng., *et al*. is another detection approach for SSI developed to overcome this drawback of the method in [18]. Thispaper developed a different approach to produce the mining dataset with its size significantly reduced. This paper also verified that the method proposed in [20] runs more efficiently in term of running time as well as the approach for SSID more effectively.

[21] by L. Wang., *et al*. developed an efficient algorithm for eliminating most of the RTT outliers of the captured packets in the Internet environment and then proposed an improved detection approach for SSI based on a revised version of the k-Means clustering algorithm. However, this paper did not provide any analysis whether the proposed detection method for SSI is resistant to hackers' session manipulation with either time-jittering or chaff-perturbation. The network experiment conducted in this paper verified that the k-Means clustering based approach for SSI with most RTT outliers removed can achieve an effective rate as high as 85.7% even in the Internet environment.

Another outlier detection and removal approach was proposed in [22] by O. Alghushairy., *et al*. and could be applied to detection algorithm design for network intrusion detection. This outlier de-

tection algorithm can work effectively as well as efficiently without using prior data distribution knowledge of the given dataset. However, this outlier detection algorithm also has limitations as its detection accuracy is not high in processing and mining data streams.

Conclusion

In this paper, we conducted a survey on most of the significant detection algorithm proposed for SSID in the literature with the inclusion of all recent progress in SSID. We put all these SSID methods into two different categories: host-based and network-based approaches, based on the number of the hosts used for the detection. For each of the SSID algorithms we reviewed, the key ideas used in the detection algorithm design, the advantages and issues with the algorithm, and differences among the similar SSID algorithms were discussed and presented. I believe that this review paper can help researchers in this area better understand those important SSID methods proposed in the literature aswell as develop more innovative approaches for SSID in the future.

Acknowledgment

This work of Drs. Lixin Wang and Jianhua Yang is supported by the National Security Agency NCAE-C ResearchGrant (H98230-20-1-0293) with Columbus State University, Georgia, USA.

Conflicts of Interest

The authors of this paper declare no conflict of interest.

Bibliography

1. Staniford-Chen S and Heberlein L T. "Holding intruders accountable on the internet". In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 8-10 May (1995): 39-49.
2. Zhang Y and Paxson V. "Detecting Stepping-Stones". In Proceedings of the 9th USENIX Security Symposium, Denver, CO, USA, 14-17 August (2000): 67-81.
3. K Yoda and H Etoh. "Finding a Connection Chain for Tracing Intruders". Proc. 6th European Symposium on Research in Computer Security, Toulouse, France (2000): 31-42.
4. D Donoho., *et al*. "Multiscale stepping-stone detection: Detecting pairs of jittered interactive streams by exploiting maximum tolerable delay". in the 5th International Symposium on Recent Advances in Intrusion Detection, Lecture Notes in Computer Science (2002).
5. A Blum., *et al*. "Detection of Interactive Stepping-Stones: Algorithms and Confidence Bounds". Proceedings of International Symposium on Recent Advance in Intrusion Detection, Sophia Antipolis, France, September (2004): 20-35.
6. He T and Tong L. "Detecting Encrypted Stepping-Stone Connections". *IEEE Transactions on Signal* 55 (2007): 1612-1623.
7. J Yang., *et al*. "Monitoring Network Traffic to Detect Stepping-Stone Intrusion". The Proceedings of 22nd IEEE International Conference on Advanced Information Networking and Applications (AINA 2008), Okinawa, Japan (2008): 56-61.
8. J Yang and Y Zhang. "RTT-based Random Walk Approach to Detect Stepping-Stone Intrusion". IEEE 29th International Conference on Advanced Information Networking and Applications (2015): 558-563.
9. Yang J., *et al*. "Manipulating network traffic to evade stepping-stone intrusion detection". *Internet of Things* 3 (2018): 34-45.
10. Wang L., *et al*. "A Framework to Test Resistency of Detection Algorithms for Stepping-Stone Intrusion on Time-Jittering Manipulation". *Wireless Communication and Mobile Computing* 2021 (2021): 1-8.
11. Zhang Y., *et al*. "Resist Intruders' Manipulation via Context-based TCP/IP Packet Matching". In Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA 2010), Perth, Australia (2020): 20-23.
12. Wang X and Reeves D. "Robust Correlation of Encrypted Attack Traffic through Stepping-Stones by Flow Watermarking". *IEEE Transactions on Dependable and Secure Computing* 8 (2010): 434-449.
13. Gamarra M., *et al*. "Analysis of Stepping-Stone Attacks in Internet of Things Using Dynamic Vulnerability Graphs". In Modeling and Design of Secure Internet of Things; Kamhoua, C.A., Njilla, L.L., Kott, A., Shetty, S., Eds.; Wiley: Hoboken, NJ, USA 1 (2020): 273-294.

14. Yang J. "Resistance to Chaff Attack through TCP/IP Packet Cross-Matching and RTT-based Random Walk". In Proceedings of the 30th IEEE International Conference on Advanced Information Networking and Applications, Crans-Montana, Switzerland, 23-25 March (2016): 784-789.

15. H Clausen., *et al*. "Evading stepping-stone detection with enough chaff". in Network and System Security (2020): 431-446.

16. Yung KH. "Detecting Long Connecting Chains of Interactive Terminal Sessions". In Proceedings of the International Symposium on Recent Advance in Intrusion Detection (RAID), Zurich, Switzerland, 16-18 October (2002): 1-16.

17. J Yang., *et al*. "A Real-Time Algorithm to Detect Long Connection Chains of Interactive Terminal Sessions". Proceedings of 3rd ACM International Conference on Information Security (Infosecu'04), Shanghai, China, November (2004): 198-203.

18. Yang J and Huang, SHS. "Mining TCP/IP packets to detect stepping-stone intrusion". *Computers and Security* 26 (2007): 479-484.

19. Wang L., *et al*. "Detect Stepping-stone Intrusion by Mining Network Traffic using k- Means Clustering". In Proceedings of the 39th IEEE International Performance Computing and Communications Conference (IEEE IPCCC 2020), Austin, TX, USA, 6-8 November (2020): 1-8.

20. Sheng Y., *et al*. "Mining Network Traffic Efficiently to Detect Stepping-Stone Intrusion". In Proceedings of the 26th IEEE International Conference on Advanced Information Networking and Applications, Fukuoka, Japan, 26-29 March (2012): 862-867.

21. Wang L., *et al*. "Effective algorithms to detect stepping-stone intrusion by removing outliers of packet RTTs". *Tsinghua Science and Technology* 27 (2021): 432-442.

22. Alghushairy O., *et al*. "Improving the Efficiency of Genetic-Based Incremental Local Outlier Factor Algorithm for Network Intrusion Detection. Advances in Artificial Intelligence and Applied Cognitive Computing". In Transactions on Computational Science and Computational Intelligence; Arabnia, H.R., Ferens, K., Fuente, D., Kozerenko, E.B., Olivas, J.A., Tinetti, F.G., Eds.; Springer, Cham: New York, NY, USA. 1 (2021): 1011-1027.