An Intrusion Detection System and Attack Intension Used in Network Forensic Exploration

Saswati Chatterjee(✉), Lal Mohan Pattnaik, and Suneeta Satpathy

Faculty of Emerging Technologies, Sri Sri University, Cuttack, Odisha, India
cshiva68@gmail.com, lalmohan.p@srisriuniversity.edu.in

Abstract. Cyberattacks are occurring increasingly frequently as cyber science advances and people utilize the internet and other technology on a regular basis. Digital forensics is used to assess malicious evidence found in a network or system and compile it in a fashion that may be used in court. Network forensic analysis is a method for looking through intrusion data received from a networked environment in order to spot suspicious entities. Utilizing intrusion detection systems (IDS), such as Snort and Wireshark, is the initial step in spotting and reporting a network flooding attack.

As technology has advanced and its use has significantly expanded, there is a higher likelihood of attacks on computer networks. In order to help with the identification and/or prevention of such assaults, many techniques have been developed. One well-liked technique is the use of network intrusion detection and prevention systems or NIDS. Businesses can choose from a variety of open-source and commercial intrusion detection systems nowadays, but the fundamental problem is still their performance. An intrusion detection system's job is to safeguard a network against risks posed by security experts, hackers, and crackers as well as the possibility of unlawful activities. A network administrator needs to develop their signature and keep up with new attack types because issues might arise when new attacks appear quickly. IDS would monitor network traffic and only compare packets that included signatures from its own signature database or traits of known failed attacks in the past.

Keywords: Network Forensic · Intrusion Detection System · Attack Analysis · Attack Intention

1 Introduction

Computer technologies expand the capabilities of computers [1, 2]. This technique is used by hackers to steal data from networks. As a result of misuse or criminal activity utilizing networks, many third parties suffer yearly losses in the billions of dollars. The frequency and calibre of attacks from viruses, worms, spam, and denial-of-service (DoS) on networks worldwide increased. These are categorized as cybercrime.

Firewalls, intrusion detection systems (IDS), and antivirus software are just a few examples of the tools that private users and organizations use, but criminals are also

S. Nandan Mohanty et al. (Eds.): ICISML 2022, LNICST 470, pp. 334–345, 2023.
https://doi.org/10.1007/978-3-031-35078-8_28

growing more intelligent and sophisticated in how they carry out their acts [3]. On the other side, failure to identify and deal with offenders right away introduces a problem. Most network administrators found their computer/network intrusions after the incident was resolved.

Security could be a big issue for all networks in the company nowadays. Numerous hacking and intrusion attempts to obstruct company processes and network services have been effective. Most network administrators detected their computer/network intrusions after the situation was handled. The attacker typically altered or eliminated the evidence required to carry out loss prevention in attacks where the system administrator was not present. In the event that a safety mechanism is unable to stop and promptly detect the attack, a security system supplement that can monitor, gather, and preserve digital evidence is required. An inquiry is carried out to ascertain the issue's breadth. The majority of the time, the computers under investigation are either used for illegal behaviour or are intended to be the targets of it. People who attack computer systems all across the world are found and prosecuted with the aid of computer forensics As a result, when conducting a forensics investigation, the legislation must be meticulously observed. Knowing who committed the crime is not enough; a forensics investigation must be conducted to ensure that the evidence obtained is admissible in court.

Digital forensics is the application of inspection and analysis methods to collect and preserve data from appropriate computer equipment in a format that may be presented as evidence in court [4]. Network forensics, a subfield of digital forensics, studies the information flow on computer networks to acquire data, compile evidence for a case, or identify intrusions. It involves gathering, storing, and researching data about network events. Other names for it include mining and packet forensics [5]. Snort is an intrusion detection system with rules that can recognize almost any type of attack and a modest but effective detection engine. In addition to its large rule sets, its flexibility enables us to define our own rules [6]. An efficient and well-known packet tool set, Snort is a signature-based network intrusion detection and prevention system. The usage of rules, some of which are preloaded, is what gives Snort its power, but we can also create specialized rules that only send alerts or block certain network traffic when the required conditions are fulfilled [7].

Real-time traffic analysis and packet logging are features of the open-source network-based intrusion detection/prevention system (IDS/IPS) based on Snort that is used on Internet Protocol (IP) networks. Protocol analysis, content searching, and matching are all done with Snort [8, 9]. The real-time collection and presentation of packets in a comprehensible format are done using a network analysis program called Wireshark. In Wireshark, you can use filters, colour coding, and other tools to examine specific packets and analyse network data. Network forensics, software development, and analysis are some of the methods in network inquiry that are most frequently utilized. [10].

Unfiltered USB communication is captured. TShark, a command-line alternative to Wireshark, is available in addition to having a graphical user interface for analysis. [11]. According to Fang-Yie et al. [12], the majority of laptop systems now use user IDs and passwords as login patterns to verify users. However, because many users share their login information with co-workers and ask for their assistance with cotasks, the pattern is one of the weakest areas in laptop security.

Zhang et al. [13] use the TrueCrypt application in two different scenarios: one is to help a private user recover a forgotten password, and the other is to conduct a computer forensic investigation of criminal activities. The computer forensic for Truecrypt encrypted volumes includes both normal and hidden volumes. The mechanism of password verification and Truecrypt encryption being explicitly demonstrated. A variety of technologies can be used to collect digital evidence using the data structure that is now in memory. They also suggested using a tool called Cafegrid, which runs on both Windows and Linux and can be used to conduct in-depth analysis and retrieve data from memory.

2 Network Forensic

Network forensics is a process for gathering, storing, and examining information about network behavior. It is used to determine the root cause of security breaches and other systemic information security issues. Network forensics' fundamental objective is to identify all potential security breach sources and develop solutions for loss minimization through early detection and intervention [1]. In order to maintain the network, the network administrator cannot solely rely on IDS. In order to thoroughly examine the incident and protect the network from threats or assaults, administrators also require an audit tool and an investigative methodology.

The capacity of the forensic network to reproduce the scenario in a system that records all data traffic activity on the network allows investigators to conduct their investigations by evaluating past events and assessing present ones. According to the aforementioned requirements, a network forensics system should use at least some of the following techniques:

1. The observation and data gathering for a network utilization audit, including traffic, capacity, and data content Therefore, monitoring and data storage systems that might be utilized as digital evidence were necessary for any network forensic system.

   Analyzing the informational content Not all of the stored data are a threat to the security of the system, thus the necessary data analysis can determine which data are compromising the security of the system. Due to the possibility that the data being examined contain personal information, it also addresses privacy-related issues.

2. Source traceback: In order to reduce the likelihood of future attacks on network security systems, it is required to use the necessary techniques to identify the attack's origin.

3 Intrusion Detection System

An intrusion detection system keeps track of suspicious activity on a network system and network traffic IDS will notify the system or network administrator if it detects any suspicious behavior regarding network traffic. A user or IP address is commonly prevented from acting in response to strange or unexpected traffic by IDS.IDS came into existence with a wide range of types and a distinct methodology that mainly functions to identify suspicious network traffic. IDS examples include host-based and network-based (NIDS) (HIDS). An IDS finds the search based on recognizable characteristics of the

trials that are consistently executed. Similar to how antivirus software recognizes and thwarts assaults, this strategy. There is also the IDS, which detects irregularities in traffic flow by comparing the current usual traffic patterns.

IDSs can also be used to provide evidence in criminal and civil legal procedures, while their primary goal is to identify intrusions and trigger evasive actions The main objective of intrusion detection is to locate, ideally in real-time, instances of illegal access to, use of, and abuse of computer systems by both internal and external intruders. Intrusion detection is founded on the theory that anomalies that may appear in a system are signs of improper, intrusive, or criminal activities in the event of anomalous intrusions.

However, the ultimate objective with regard to a forensic application would be to gather enough proof to link the crime to the offender. The inherent anonymity that a criminal has within a computer system encourages damaging behaviour while making it very challenging for law enforcement to identify the offender. In order to get a handle on identifying the offender, it is crucial to be able to create a fingerprint of system users and their regular behaviour.

The analysis of access log files will always be used as a cornerstone of the evidence-gathering process. At a higher level, it is frequently required to have a more thorough capacity to reduce the field or even create a list of potential suspects. Computer crimes, whether committed by system users or outsiders, are, as we all know, invariably the outcome of human activity on a system. Therefore, at this level, it is preferable to have some logging activity to provide evidence as well as some mechanism to compile and gather user profiles for the system. Computer forensics investigators can use intrusion detection systems as a place of departure.

4 Related Work

Based on the actions of cybercriminals, attack intention analysis deduces the purpose of an attack. In addition to giving more information about the cybercrime's proof and the attacker's conduct, which facilitates the identification of the offender.

According to [14], when an attack is expected and the attacker's intended target is known, attack intention is identified. Determining the underlying goals of current cyberattacks is becoming more and more difficult due to their complexity. Even specialists have trouble figuring out the entryway [15]. An attacker employs tools to hide or camouflage his patterns from his victims and follows a logical set of steps to complete his purpose. According to Huang et al. [16], pattern recognition is more difficult in network systems with a variety of attack tactics. For instance, false positive or false negative reading errors are the main problem in IDS, especially in misuse-based and anomaly-based detection, as described by [17–19]. The limitations of security sensors and network monitoring technologies, in summary, make attack observation imprecise and challenging to comprehend [25]. The attack trees can be analyzed to forecast a group of attack libraries that are related to the attack graphs and represented by a collection of graphs.. This method's manual implementation makes it typically time-consuming.

The alternate method builds the attack automatically using a graph from the checking model [22]. The strength of this paradigm, according to Qin and Lee [20], is its effectiveness in evaluating protocols. This paradigm has restricted scalability but is also more

reliable than other approaches like simulation or theorem methodologies. The approach [21] employs rely on figuring out the attack's goal from the attack path. The researchers presented a method for creating attack path graphs in order to identify invasive intentions. They arrived at the conclusion that the suggested strategy is inadequate and only catches the initial phases of attack intention. The researchers also found that the attack's vulnerability is dependent on its goal, demonstrating that the method is inadequate for large volumes of data.

5 Network Forensics' Detection of Intentions

To make a more accurate determination, investigators take into account a variety of prediction criteria, such as attack aim and tactics. Analysis of attack intent as a predictive element aid in hastening the decision-making process for apprehending the actual offender. However, the majority of the methods now in use for attack intention analysis concentrate on identifying the alert correlation between certain pieces of information.

The attack intention analysis, which focuses on the justification for ambiguous intentions, is presented in this section. In this phase, the attack intention analysis model from [23] is enhanced and introduced. A new model that predicts attack intents by fusing the probabilistic technique of a causal network with the mathematical D-S evidence theory is also presented.

The set of procedures used to determine attack intents is shown in Fig. 1, which is an improvement over the model suggested in [23]. The stated methods must be followed in order to identify the assault type. To establish the relationship between the acquired data, attack features should be developed. Before examining attack intents, this group of procedures needs to be specified. In general network forensics [31], the preparation, detection, collecting, and assessment of evidence processes should be predefined as previously indicated.

Predictions of attack intentions are influenced by the nature of the attack, which is determined based on the attack evidence. A range of security sensors and detection system devices are used to identify attacks (both commercial and non-commercial security products, such as IDS). The type of attack depends on how accurate these items are. The proposed process model assumes that the attack is precisely located and recognized. This paradigm assumes that the detection tools—open-source or commercial, like Kaspersky or Snort—were utilized to find the attack. The percentage of attacks that are accurately identified is calculated by averaging all detection rates based on detection techniques.

The attack intention analysis (AIA) technique that was released can be understood using the given model.

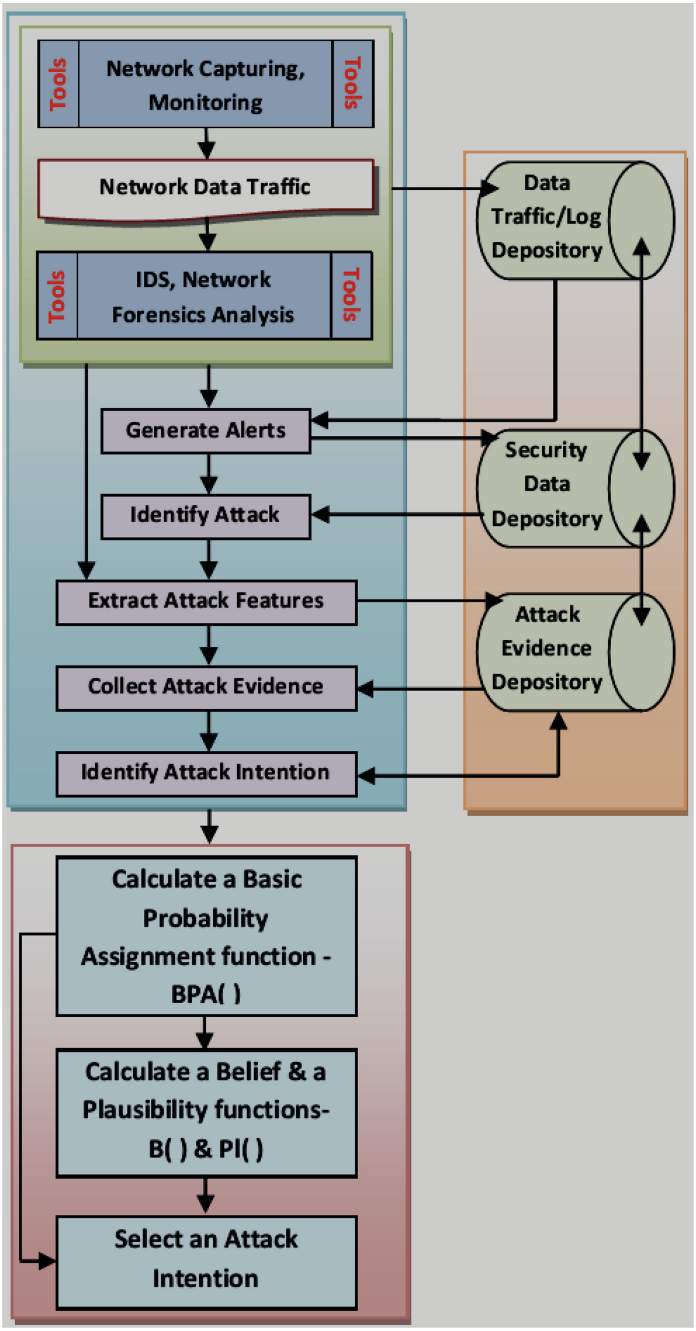

Fig. 1. Using D-S Evidence, a Model of the Attack Intention Process

6 Proposed Work

6.1 Data Monitoring

A forensic process is done in a number of steps. It is All network data flow can always be observed, recorded, and stored by a network forensics system. Attacks on systems connected to the Internet network are possible. As a result, it is essential to implement an Intrusion Detection System monitoring and detection mechanism for network threats. An IDS system has the ability to collect data, analyse that data to look for anomalous network activity, and then communicate the results of that analysis and detection process. There are two types of intrusion detection algorithms. The first uses signature-based detection as its foundation. Attacks are detected using signature-based detection by using an example of a previously saved attack pattern. The second step is anomaly detection, which establishes if a departure from typical usage patterns qualifies as an incursion.

6.2 Data Analysis

Network forensics makes it possible to examine and analyze previously saved data. Potential sources of evidence for computer and network forensics are numerous. The document may contain proof.. Backups, caches, historical data, and activity logs can all be stored in the output of various programs, including word processors and spreadsheets. The incidence of threats or network attacks, on the other hand, may be revealed by monitoring network activity, which may retain some valuable information. Network activity that can show illicit conduct that was more thoroughly documented than other sources. Consequently, a crucial source of potential evidence is the system log. A business or organization should keep records of all network operations, including computer-based logins and the use of remote Telnet or FTP. The tape may contain a range of information about a specific user's activities, including the event date and time, which makes it very helpful in the investigation. Internal factors, such as email and online access, as well as exterior factors that could provide evidence of the event's timing, are involved (timeline). A timeline connects the various events that are entered into a system to an allegation and also establishes an alibi and identify the independent crime proof.

6.3 Centre Track

To selectively transfer datagrams back from the outer edge router to the specialized router tracking, a network overlay IP tunnel called Center Track is employed. An IP tunnel can be constructed on an IP network. When the attack starts at or goes through the prior hop, 8an analysis tool called input debugging will show it. An overlay network is used to channel traffic made for dynamic routing that only impacts the victims. Tracking is done hop-by-hop, beginning with the router closest to the victim (Fig. 2).

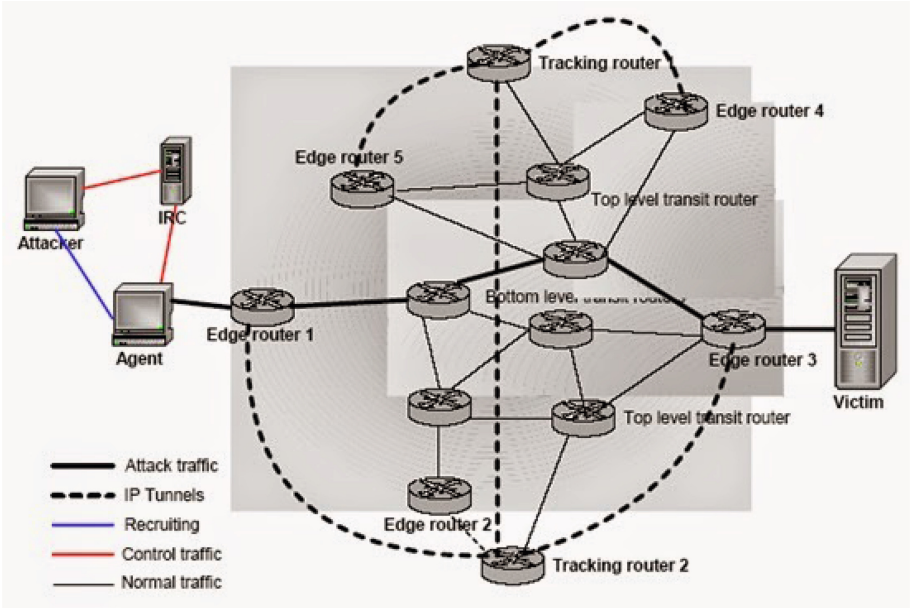

Fig. 2. Center Track scheme

Tracing a Sleepy Watermark

In order to conduct traceback using the primary chain relationships, Sleepy Watermark Tracing (SWT) was developed. This method can be used to identify an attacker when a computer-controlled remote control is used as the slave machine. The SWT-guarded host and the SWT-guarded gateway are the two components of the SWT architecture (Fig. 3). Applications that support IDS and watermarks are employed as a supporting element on the SWT-protected host. The SWT tracing process is started by IDS. IDS connects to SWT subsystems via the SWT-protected host when an intrusion is found and launches a watermark tracing.

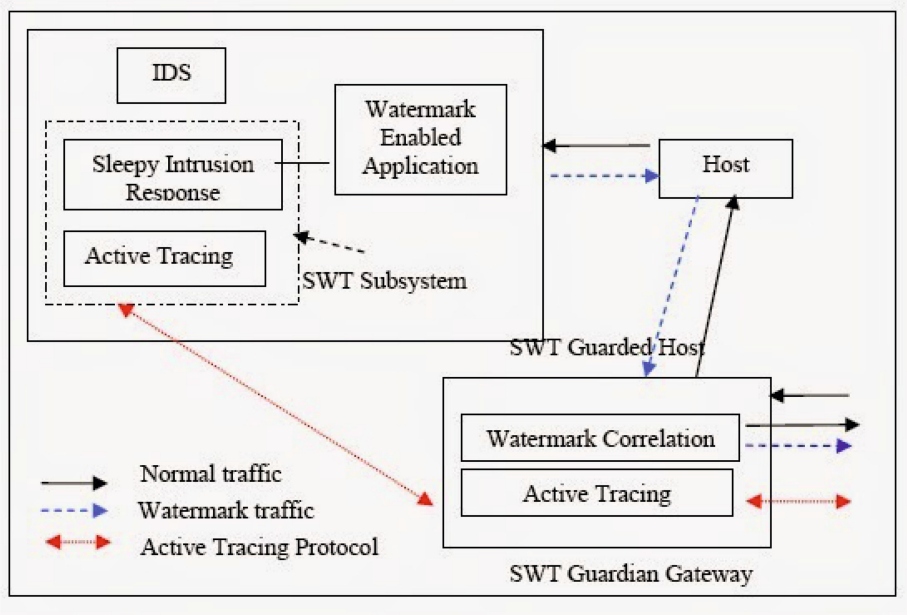

Fig. 3. Architecture of SWT

7 Comparison Findings

Without evidence, neither the intention of an attack nor its resolution can be shown [18, 24]. On the one hand, the probability of believing that a single piece of evidence represents an actual attack intention will not be as precise as when the evidence is integrated with other evidence if the AIA algorithm gathers a single piece of evidence for each intention. On the other hand, if an attack intention is supported by more evidence, there is a greater chance that the attack will really occur, increasing the accuracy of the intention.

Results from [24] show that the backdoor attack was accurately detected with 98.68% accuracy. The outcome indicates that, with a 0.595856914 likelihood ratio, the likely attack purpose was to spy on the users of the infected devices (spying) and to further propagate the virus by automatically scanning the whole network range and propagating the infection via vulnerabilities. The accuracy of the attack intention detection probability ratio is 0.788. The following equation is used to calculate this accuracy value:

$$\text{Accuracy} = (\text{TPDR} + \text{TNDR}) / (\text{TPDR} + \text{TNDR} + \text{FPDR} + \text{FNDR})$$

where

The percentage of all correctly predicted attack intentions is known as accuracy.
The ratio of an assault that is correctly identified is known as TPDR.
The ratio of attack intention that is accurately identified is known as TNDR.
The ratio of attacks that are wrongly identified (FPDR).
The ratio of improperly detected attack purposes is known as FNDR.

The majority of the above-described studies [25–27] in attack intention analysis are connected. These researchers conducted their studies on a small sample and assessed their findings using certain data, such as CVE, OS, and host services. Table 1 displays the findings of a comparison between the AIA algorithm-based attack intention analysis and other analyses. The evidence used and presented in the associated studies is the foundation for the comparison's findings.

Table 1. Comparison of the outcomes of the Attack Intention Analysis

	TPDR	TNDR	FPDR	FNDR	Accuracy (%)
(Peng et al. [18])	0.980	0.019	0.981	0.020	0.500
(Wang and Peng [18, 24])	0.980	0.019	0.981	0.020	0.500
(Wu et al. [25])	0.980	0.019	0.981	0.020	0.500
(Hao et al. [27])	0.980	0.011	0.989	0.020	0.496
(Hao et al. [27])	0.980	0.034	0.966	0.020	0.507
(Rasmi and Aman [20])	0.980	0.595	0.405	0.020	0.788

8 Conclusion

Network flaw-related crimes can happen anywhere. For computer system security, firewalls and IDS are no longer adequate, hence a network security system with the necessary forensic capabilities must be developed [28]. A firewall may fall for a hacker or computer virus attack. The damaged system will be further investigated by network forensics. Because the forensic system will violate privacy, there needs to be a legal system policy that will be upheld by a business or organization. There is a need to make an effort to standardize system network forensics because of the current forensic system technique and system development strategy. The entire world has moved into the digital realm as a result of the quickening pace of technological development. However, this change has also led to an increase in cybercrimes and security breach occurrences, which endanger user security and privacy [29]. As a result, this article examined how using digital forensics to fight cybercrime has been a significant advancement in cybersecurity [30, 31].

References

1. Ruchandani, B., Kumar, M., Kumar, A., Kumari, K., Sinha, A.: Experimentation in network forensics analysis. In: dalam Proceedings of the Term Paper Series under CDACCNIE. Bangalore, India (2006)
2. Meghanathan, N., Allam dan, S.R., Moore, L.A.: Tools and techniques for network. Int. J. Network Secur. Appl. **1**(1), 14–25 (2009)

3. Kang, B.-H.: A generic framework for network forensics. Int. J. Comput. Appl. **1**(11), 1–6 (2010)
4. Agarwal, R., Kothari, S.: Review of digital forensic investigation frameworks. In: Kim, K.J. (ed.) Information Science and Applications. LNEE, vol. 339, pp. 561–571. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46578-3_66
5. Marcus, R.: Network Forensic Analysis Definition (2019). www.wikipedia.com/networkforensics. Accessed 26 Feb 2022
6. Jaw, E., Wang, X.: A novel hybrid-based approach of snort automatic rule generator and security event correlation (SARG-SEC). PeerJ Comput. Sci. (8)900 (2022). https://doi.org/10.7717/peerj-cs.900
7. William, S.: Quality of service and quality of experience: network design implications, with florence Agboma. Internet Protocol J. **13**(7), 251–269 (2016)
8. Carta, S., Podda, A.S., Recupero, D.R., Saia, R.A.: Local feature engineering strategy to improve network anomaly detection. Future Internet **12**, 177 (2020)
9. Yang, C., Chung-Huang, Y.: Fast deployment of computer forensics with USBs. In: Proceedings of the 2010 International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 413–416 (2010). https://doi.org/10.1109/BWCCA.2010.106
10. Zhang, K., Zhao, F., Luo, S., Xin, Y., Zhu, H.: An intrusion action-based IDS alert correlation analysis and prediction framework. IEEE Access **7**, 150540–150551 (2019). https://doi.org/10.1109/ACCESS.2019.2946261
11. Nitin, V.: Detect network threat using SNORT intrusion detection system. Int. Res. J. Eng. Technol. **09**(01), 61–66 (2022)
12. Mandeep, K., Navreet, K., Suman, K.: A literature review on cyber forensic and its analysis tools. Int. J. Adv. Res. Comput. Commun. Eng. **1**(5), 23–28 (2016)
13. Fang-Yie, L., Kun-Lin, T., Yi-Ting, H., Chao-Tung, Y.: An internal intrusion detection and protection system by using data mining and forensic techniques. In: International Conference on Availability, Reliability and Security, pp. 1932–8184. Taiwan (2015)
14. Zhang, L., Yu, Z., Jia, Q.F.: The forensic analysis of encrypted truecrypt volumes. Computer Science. In: IEEE International Conference on Progress in Informatics and Computing (2014)
15. Wei, W., Thomas, E.D.: A graph based approach toward network forensics analysis. ACM Trans. Inf. Syst. Secur. **12**(1), 1–33 (2008)
16. Huang, M.-Y., Jasper, R.J., Wicks, T.M.: A large scale distributed intrusion detection framework based on attack strategy analysis. Comput. Netw. **31**(23–24), 2465–2475 (1999)
17. Qin, X., Lee, W.: Attack plan recognition and prediction using causal networks. In: Computer Security Applications Conference (2004)
18. Peng, W., Yao, S., Chen, J.: Recognizing intrusive intention and assessing threat based on attack path analysis. In: Multimedia Information Networking and Security, International Conference (2009)
19. Bonnie Brinton, A., James, V.H., Paul Benjamin, L., Scott, L.S.: The application of model checking for securing e-commerce transactions. Commun. ACM **49**, 97–101 (2006)
20. Rasmi, M., Jantan, A.: Attack intention analysis model for network forensics. In: Zain, J.M., Wan Mohd, El-Qawasmeh, E. (eds.) ICSECS 2011. CCIS, vol. 180, pp. 403–411. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22191-0_35
21. Pilli, E.S., Joshi, R.C., Niyogi, R.: Network forensic frameworks: survey and research challenges. Digit. Investig. **7**(1–2), 14–27 (2010)
22. Rasmi, M., et al.: Attack intention analysis model for network forensics. In: Zain, J.M., Wan Mohd, W.M.b., El-Qawasmeh, E. (eds.) Software Engineering and Computer Systems. ICSECS 2011. CCIS, vol.180. Springer, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-22191-0_35

23. Rasmi, M., Jantan, A.: AIA: attack intention analysis algorithm based on d-s theory with causal technique for network forensics - a case study. Int. J. Digital Content Technol. Appl. **5**(9), 230–237 (2011)
24. Wang, Z., Peng, W.: An intrusive intention recognition model based on network security states graph. Wireless Communications, Networking and Mobile Computing (2009)
25. Wu, P., Zhigang, W., Junhua, C.: Research on attack intention recognition based on graphical model. In: Information Assurance and Security (2009)
26. Feng, J., Yuan, Z., Yao, S., Xia, C., Wei, Q.: Generating attack scenarios for attack intention recognition. In: International Conference on Computational and Information Sciences. IEEE Computer Society, Chengdu, China (2011)
27. Hao, B., Kunsheng, W., Changzhen, H., Gang, Z., Xiaochuan, J.: Boosting performance in attack intention recognition by integrating multiple techniques. Front. Comput. Sci China **5**, 109–118 (2011)
28. Samantaray, M., Satapathy, S., Lenka, A.: A systematic study on network attacks and intrusion detection system. In: Skala, V., Singh, T.P., Choudhury, T., Tomar, R., Abul Bashar, M. (eds.) Machine Intelligence and Data Science Applications. Lecture Notes on Data Engineering and Communications Technologies, vol. 132. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-2347-0_16
29. Potluri, S., Mangla, M., Satpathy, S., Mohanty, S.N.: Detection and prevention mechanisms for DDoS attack in cloud computing environment. In: 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1–6 (2020). https://doi.org/10.1109/ICCCNT49239.2020.9225396
30. Alghamdi, Md.: Digital forensics in cyber security -recent trends, threats, and opportunities (2020)
31. A Hybrid Approach for Network Intrusion Detection by Ganesh Prasad Rout, Sachi Nandan Mohanty. In: Fifth IEEE International Conference on Communication Systems and Network Technologies, pp. 614–617 (2015), ISBN 978-1-4799-1797-6/15