Journal of Engineering Science and Technology
Vol. 16, No. 4 (2021) 3534 – 3547

NIPSA INTRUSION CLASSIFICATION

MOHAMMED NADIR BIN ALI[1,*], MADIHAH MOHD SAUDI[2], TOUHID BHUIYAN[1], AZUAN BIN AHMAD[2], MD. NAZRUL ISLAM[1]

[1]Daffodil International University, Dhaka, Bangladesh
[2]Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai, Malaysia
*Corresponding Author: mdnadir@daffodilvarsity.edu.bd

Abstract

With the extensive growth of the Internet, network security has become more important. The growing proportion of network intrusions has impacted network security more than ever. The number of network attacks is significantly increasing. One major method of defence against these attacks is the intrusion detection and prevention system. For an in-depth understanding of this system, a conceptual framework for intrusion classification must be developed. This classification framework could be used to develop the algorithm for a Network-based Intrusion Detection System (NIDS) and a Network-based Intrusion Prevention System (NIPS). Up until this point, a structured framework or standard for classifying network intrusion has limitations to identify the intrusion. To comprehend the threats posed by intrusion, this paper proposes a new way for classifying network intrusion efficiently. Experimental results indicate that the proposed NIPSA intrusion classification can identify intrusion with an overall rate of accuracy of 99.42%, a 0.3% FP rate, and a 0.6% FN rate. The NIPSA intrusion classification can help organizations to implement Network-Based Intrusion Detection and Prevention System for better performance in the future.

Keywords: Intrusion, Intrusion classification, Network security, NIDS, NIPS, NIPSA.

1. Introduction

A network intrusion can be extremely devastating to an organisation, as company documents personal information, and other sensitive data can be stolen as a result of intrusions. It is impossible to fully prevent a network intrusion. Preventing intrusion can be done by disabling the network connections, disconnecting the affected systems, and creating and applying access control lists for firewalls and routers. However, these measures are not good enough to secure the network and save valuable data from intrusion. To protect computer networks from network intrusions, there is a need to detect and prevent possible intrusion attempts. In particular, an effective and reliable intrusion prevention model that is capable of preventing the potential attack in real-time must be developed.

Karatas and Sahingoz [1] developed network-based intrusion detection systems with different training functions based on neural network. Ali [2] has developed Network-Based Intrusion Prevention System Inspired by Apoptosis and used CICIDS2017 in the paper. Moreover, a reliable approach for anomaly network-based IDS was proposed by Mazini et al. [3]. Network security comprises three key principles of security: (i) confidentiality (ii) integrity and (iii) availability [4]. Depending on the application and context, one of these principles might be more important than the other. The principles of security help to determine security threats in organizations. These security principles are elaborated below.

In network security, confidentiality refers to the protection of information by limiting the access and disclosure of information to an unauthorized source. Confidentiality is the user's ability to access different information and resources in a definite location in a specific format [5]. It implies keeping information private. This is the part of network security that ensures that those who are authorized to access information can do so while preventing access to unauthorized persons. Privacy could involve physically or logically restricting access to sensitive information applying appropriate credentials to access specific network resources or the encryption of traffic traversing a network.

The integrity of data is a critical component of information security, especially in industries with highly sensitive data [6]. Integrity refers to another network security concept of information protection, which aims to maintain and ensure the accuracy, consistency, and trustworthiness of information. The function of integrity is to make sure that information has not been modified or destroyed by unauthorized persons or hackers. Ensuring integrity is ensuring that the data sent from the sender is the same as the data received by the recipient without any change in information.

The availability of information in network security refers to the protection of information systems from unauthorized disruption. It also indicates the up-time maintenance of all resources of information. The function of availability is to make sure that the information, network services or resources are continuously available to the intended users.

A network intrusion is any unauthorized activity in a computer network. Network intrusion can cause millions of dollars of damage by infecting computer networks in a very short time. The top network attacks in 2018 are shown in Fig. 1.

Intrusions are the attacks that succeed. Therefore, the term attack represents both successful and attempted intrusions [7].

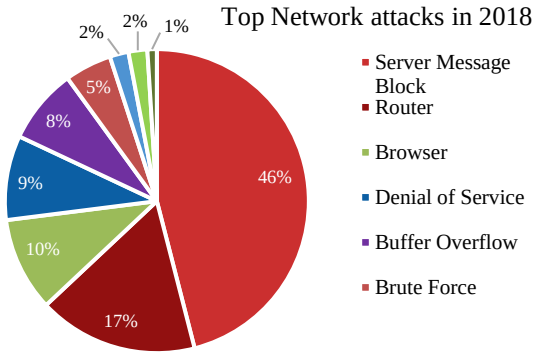

Fig. 1. Top Network Attacks in 2018 [7].

An intrusion prevention process is an important part of network functions in this age of rapidly changing computer technology. It is very difficult to imagine the extent of the cost incurred in response to all intrusion incidents occurring in one country.

Figure 2 shows the average estimated costs of Cybersecurity breaches in different business companies. It was identified that the estimated total cost of breaches has consistently increased for small business £1,210 and for all businesses £1, 410 in the year 2018 to 2019 (Rishi, 2019). It is worth noting that the lack of certainty around the likely cost of any breach can make it difficult for businesses to fully understand the return on investment in Cybersecurity.

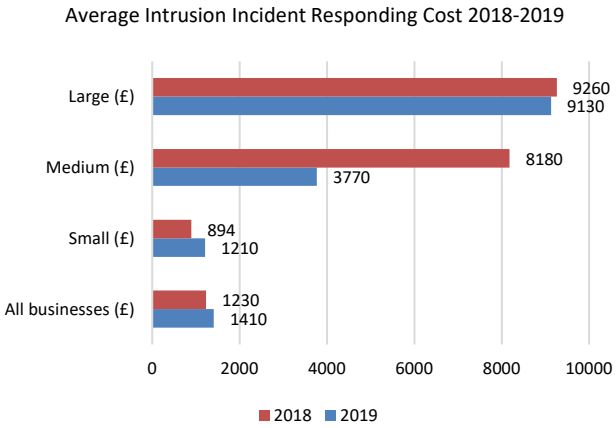

Fig. 2. Average cost of responding to intrusion incidents from 2018-2019 [8].

The objective of this paper is (i) to propose an intrusion classification (ii) to compare existing work with the proposed intrusion classification (iii) to improve the proposed intrusion classification accuracy. The contribution of this paper will help researchers to implement Network-Based Intrusion Detection and Prevention System for better performance in the future.

2.2. Related work

A network intrusion is any unauthorized activity on a computer network. It is a critical challenge plaguing information and communication systems amongst other forms of fraud perpetrated over the Internet [9]. Many researchers have discussed different ways of classifying computer network attacks. The current taxonomy classifies attacks based on the transitions made between privilege levels and actions performed [10]. By incorporating these taxonomies, the attacker will be able to achieve unwanted access to the computer network system [11]. Howard [12] classified attacks according to the Attacker, the Tool, Access, the Result, and the Objective. Salvatore et al. [13] mentioned four main intrusion categories: (i) DoS (ii) R2L (iii) U2R and (iv) Probing. In his thesis, Kumar [14] introduced a method of classification based on attack signatures used within IDS IDIOT. Saudi et al. [15] introduced STAKCERT worm classification consisting of five main attributes: (i) infection (ii) activation (iii) payload (iv) propagation and (v) operating algorithm. Khaleel et al. [16] classified security attacks into two: (i) passive and (ii) active.

Intrusion analysis entails analysing each network packet that passes over a network to detect and monitor intrusive activities and behaviour. These steps involve the techniques given in Fig. 3.

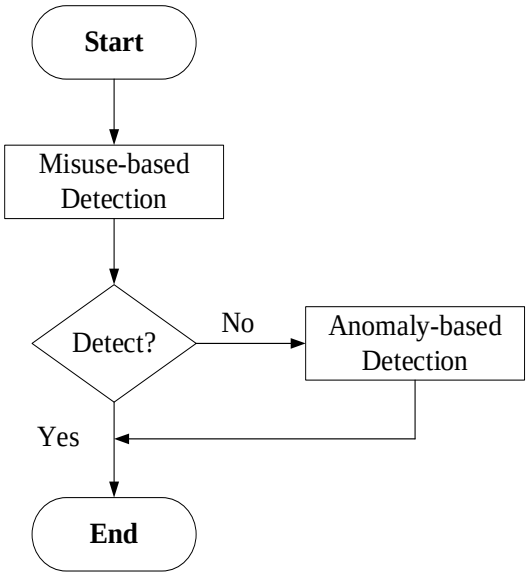

Fig. 3. Intrusion analysis.

- **Misuse Analysis**

In this section, misuse analysis is discussed. The alternate name for misuse detection is signature-based detection. Signature-based detection looks for specific patterns, such as, byte sequences in a packet, or known malicious instruction sequences used by malware. Signature-based detection monitors a packet in the network and compares it with pre-configured and pre-determined

attack patterns called signatures. To conduct a misuse analysis, a raw socket is used for sniffing the packet. Scapy is used for decoding, and YARA is used for matching the signature. The whole process is developed in Python.

- **Behavioural Analysis**

Behavioural analysis involves examining network traffic to identify intrusion, which leads to abnormal network traffic, unwanted violations of security policies, and some malware. It involves the collection of events generated by the user, the host, and the network. Activities that are not benign are assumed to be intrusions. Behavioural analysis creates a profile that represents normal behaviour collected from historical data over some time when things behave "normally". This analysis builds a model of benign activities in a network and is used to predict the expected state of the network, which is later compared with the current state. An alert is then raised when the measured value differs from a specific threshold significantly. For the behavioural analysis, different tools are used, e.g., Wireshark, Snort, ntopng, to suit certain parameters of network behaviour.

3. Lab Architecture

The architecture of the lab for testing in this paper is shown in Fig. 4. It is an organized lab atmosphere in which more than 80% open-source software was used for testing. The lab architecture was used without any Internet connectivity. The finding of the tests showed that the analysis of results and problem fixing could be done instantly.

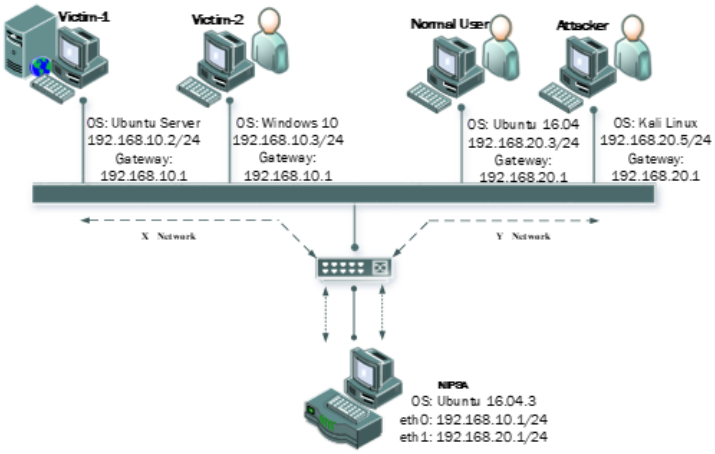

Fig. 4. Lab architecture.

4. Intrusion Classification

Nowadays, Internet security is a vital issue in the Cyberworld [16]. Intrusion is a violation of security policy. Network intrusions are malicious activities that intruders execute against network security policy. The number of network intrusions is growing. Based on the network intrusion analysis in the laboratory, the researchers produced a new network intrusion classification. This classification

is based on five attributes: (i) infection (ii) propagation (iii) activation (iv) payload and (v) operating method. In this paper, the intrusion classification was produced based on STAKCERT worm classification [17], as both network intrusion and worm classification share similar attack procedures in the network. Figure 5 shows an overview of the proposed intrusion classification.

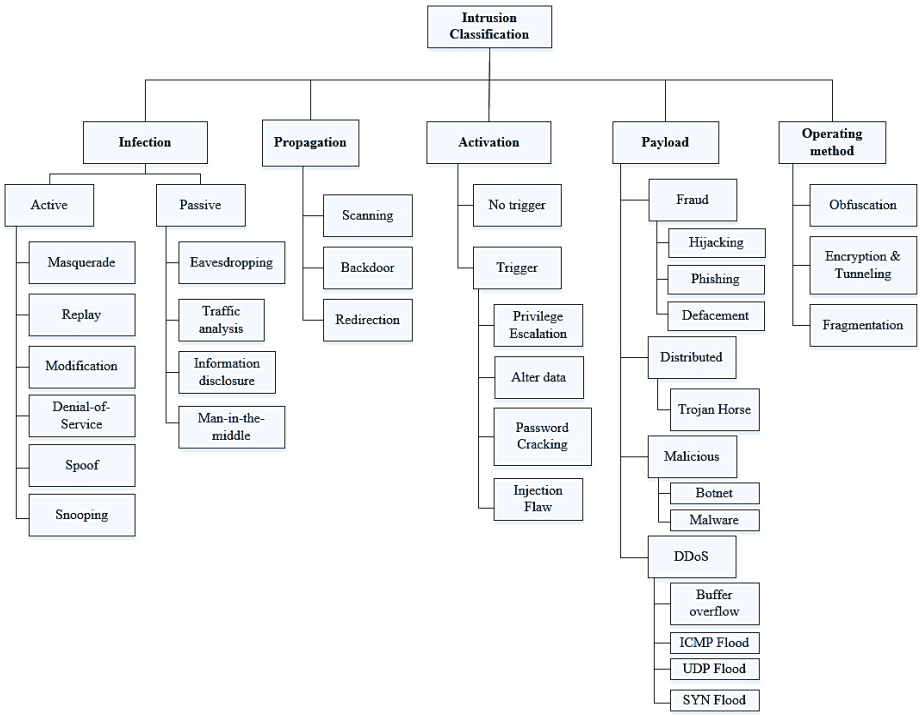

Fig. 5. Intrusion classification.

Infection is the first step in which intrusion infects a network. Propagation is how the intrusion spreads in the network. Activation is a technique that activates the intrusion. The operating method is a mechanism used to bypass detection.

I. Infection

Infection deals with how a network gets infected by an intrusion. There are two types of attack: (a) active and (b) passive.

a) Active attack

An active attack is a kind of network infection that attempts to infect an operation. Aslam et al. [18] classified active attacks into four: (i) snooping (ii) modification (iii) masquerading and (iv) denial-of-service (DoS). There are quite a few infections of this type in operation in the cyber world. Some of these types are elaborated below:

- **Masquerade**

Masquerade is an active infection that uses a false identity to gain illegal access to any computer or network system.

- **Snooping**

Snooping is a kind of masquerading intrusion. It takes the false identity of the receiver to make the network believe that the packet is from its source.

- **Replay**

A replay attack is one of the lower-tier versions of a "Man-in-the-middle" attack mechanism.

- **Modification**

In the context of network security, modification refers to altering or changing any part of the network settings and network-related information.

- **Denial-of-Service**

This attack prevents the legitimate user from accessing network resources or any other computer systems. It sends huge amounts of network traffic and floods the network, which DoS attacks accomplish very well.

- **Spoof**

In this type of attack, unauthorized persons pretend to be legitimate users and gain access to the network and steal important information [19]. A spoofing attack happens when an attacker attacks the network host to steal data.

b) Passive attack

The main aim of the passive attack is to acquire information about the target without changing the target data. This type of attack makes use of information from the system but does not affect system resources [20]. In this attack, the initial network infection rate is comparatively low.

- **Eavesdropping**

This attack is the act of secretly listening to a secret conversation, typically between hosts and networks.

- **Traffic analysis**

This attack can be used to determine the type of information being transmitted, even if the data itself is twisted.

- **Information disclosure**

This attack includes software distribution, patch level, and version numbers. With leaked information, the attacker can identify and learn the internal topology of a network.

- **Man-in-the-middle**

A man-in-the-middle attack requires three parties: (i) the sender, (ii) the man-in-the-middle and (iii) the receiver. In this situation, the victim tries to communicate with his actual receiver but the “man-in-the-middle” intercepts the victim’s communications. In such a case, the victim is not aware of the man-in-the-middle.

II. Propagation

Propagation is the intruder's ability to enter another network. There are a few types of propagation:

- **Scanning**

This method is used to identify vulnerable devices such as servers, PCs, and other peripherals that exist on networks. It refers to the use of a computer network to collect computing system-related information. Thus, an attacker can easily compromise a network or a system for undesirable purposes.

- **Backdoor**

Backdoor enables intruders to access and gain control and command of any targeted network without being detected. Intruders may use intended services or websites to execute an attack. Backdoors are often used to gain remote control or access to a network or system.

- **Redirection**

Redirection method refers to the redirection of Internet traffic to an unintended destination. There are numerous ways to execute this activity including port redirection and URL redirection.

III. Activation

Activation depends on the absence or presence of a trigger mechanism for intrusion.

a) No trigger

No trigger means that no instruction is given in a packet to carry on some malicious activities so the packet will be considered a normal packet.

b) Trigger

In this phase of activation, the trigger may be human, a scheduled process, or a self-trigger.

- **Privilege escalation**

This is the act of exploiting vulnerabilities, such as, a programming hole, a network flaw, and/or a design flaw or configuration oversight in a network and its services to gain access to resources that are normally protected from the application or user.

- **Alter data**

This process changes or modifies some of the information that passes over the network. Data alteration and data destruction are now increasing rapidly.

- **Password cracking**

Using malicious code, the password cracking process can also be done easily in a network. There are a lot of ways to crack passwords, such as by perpetrating some common techniques e.g., brute force and dictionary attack in a network.

- **Injection flaw**

Injection flaws allow intruders to perform malicious actions, such as, changing, altering, deleting, or reading confidential information that they are not allowed to carry. There are numerous types of injection flaw attacks including SQL injection,

HTML injection, Host header injection, XPath injection, XML injection, CRLF injection, and OS Command injection.

IV. Payload

A payload refers to the component of a computer virus that executes a malicious activity. Some ways of executing a payload include using an unprotected computer, opening an infected file, and executing an infected program.

a) Fraud

Fraud has increased tremendously with the rapid growth of Internet usage. This type of intrusion can be sub-classified into hijacking, phishing, and effacement.

- **Hijacking**

Hijacking is used simply to take privilege or gain access to confidential information or messages or to enable the intruders to alter any part of the conveyed information.

- **Phishing**

Phishing is sometimes used to gain a foothold in government or corporate networks as a part of a larger attack, for example, an advanced persistent threat (APT) attack.

- **Defacement**

Defacement is the act of destruction or damage in which a website is marked by intruders or attackers who want to leave a mark. Typically, website defacement is used to cover a larger crime going on behind the scenes.

b) Distributed

Another subclass of payload intrusion is called distributed intrusion. This is an explicit attempt by attackers to prevent the legitimate use of services in a network.

- **Trojan horse**

A Trojan horse is a computer program that appears harmless but uses malicious code to pass itself off as a trusted application. If a system is infected with a Trojan Horse, it will seem like an unusual activity and unexpected changes will occur even when the system is idle.

c) Malicious

A malicious attack is an attempt to forcefully abuse or take advantage of someone's computer in a network. The types of malicious attacks are discussed below:

- **Botnet**

In the context of network security, a botnet is a network of affected computers where a network is used to spread malicious activities. That is, a bot is an extensive collection of a large number of infected computer systems.

- **Malware**

Malware is the short form for “malicious software”. Malware are harmful applications designed to secretly operate on compromised systems or networks without the permission of the user. Primarily, malware targets the confidential and sensitive

information of individuals, corporate businesses or financial information for monetary gain.

d) DoS/ DDoS

Denial of service (DoS) is an attack that aims to shut down network resources. In the context of intrusion, this attack aims to modify the flow of control. There are a few types of DoS/DDoS, which are discussed below:

- **Buffer overflow**

Among the different types of denial-of-service attacks, buffer overflow is the most common. Its concept is to send a larger amount of network traffic to a network where the intruders want to keep the target resource or network busy to make it inaccessible to the normal user.

- **ICMP food**

ICMP flood refers to leveraging on misconfigured network devices by sending a large number of ICMP packets on the target network instead of a particular device. The ICMP flood attack is also known as a Smurf attack.

- **UDP flood**

This is a type of Denial-of-Service attack in which the intruder sends a large number of UDP packets to the target server on random ports, which causes overwhelm and makes the server unreachable and unresponsive to legitimate users or clients because the target network has been flooded with packets.

- **SYN flood**

A SYN flood is an attack mechanism for conducting a Denial-of-Service attack in a network server. The SYN flood exploits part of the process of the TCP three-way handshake to make a server unavailable to normal traffic by consuming all available resources on the server.

V.Operating Method

An operating method is explained as a procedure used by intruders to bypass detection. There are several types of Operating Methods:

- **Obfuscation**

Obfuscation is not an attack but a technique to hide malicious codes from detection machines. In simple terms, obfuscation just changes a readable string into an unreadable one, and, therefore, hindering the IPS from detecting the string.

- **Encryption and tunneling**

Encryption and tunnelling are another strategy involving encrypted data that can be used to avoid IPS inspection. Hackers are using encryption to bypass network security controls [21]. Encrypted intrusion passes over an SSH connection or a VPN tunnel to make it virtually impossible for IPS to inspect data. In this situation, IPS should be placed after the tunnel termination of the network.

- **Fragmentation**

In the context of network security, fragmentation is the process of breaking an attack into multiple packets. The malicious packet is divided into small fragments, which enables the intruder to bypass the network security mechanism easily.

5. Findings

The experimental results were guided by the testing of the intrusion classification model for intrusion detection. This phase was conducted using WEKA software, with 348 datasets, and each dataset containing five main features: (i) infection (ii) propagation (iii) activation (iv) payload, and (v) operating method used as input [22]. The dataset was clustered using simple k-means, as shown in Fig. 6. Clustering was performed to find a new set of intrusion categories from the datasets. In the CICIDS2017 datasets, clustering was performed to group all the datasets into different types of intrusion.

Algorithm 1: Simple k-Means Clustering

Input: Data $A = \{a_{1,\dots,}a_n\}$, the order k, max number of allowed iterations
Output: A partition $\mathcal{Y} = \{m_1, \dots, m_k\}$

$n \leftarrow 0, \mathcal{Y} \leftarrow \theta$
Initialize $\mu_i, i = 1, \dots, k$ randomly
for each $n \leftarrow n + 1$ **do**
    Assign sample a_j to the cluster with the nearest representative
    $m_i^{(n)} \leftarrow \{a_j : d(x_j, \mu_i) \leq d(x_j, \mu_h)$ for all $h = 1, \dots, k\}$
    Update the representatives
    $\mu_i^{(n+1)} \leftarrow \frac{1}{|m_i^{(n)}|} \sum_{a_j \varepsilon m_i} a_j$
    Update the partition with the modified cluster
    $\mathcal{Y}^n \leftarrow \{m_1^{(n)}, \dots, m_k^{(n)}\}$
    if $n \geq \max | \mathcal{Y}^n = \mathcal{Y}^{n-1}$ **then**
        return $\mathcal{Y}^n$
    end if
end for

Fig. 6. Simple k-Means clustering algorithm.

In terms of clustering, cluster0 is 20% of the datasets, followed by cluster1 at 30%, cluster2 at 39%, and cluster3 at 11% (Fig. 7). Cluster0 is also known as intrusion type0, while cluster1 is also known as intrusion type1, while cluster2 is intrusion type2, and cluster3 is intrusion type3. Before the clustering method, network packet analysis was conducted to verify the relationship between the five main features used as variables in the clustering method. In this paper, True Positive Rate (TPR), Overall Accuracy (OA), Precision (Pr.), Recall (Rc.), and F-Score (F1) have been used as performance metrics to measure the performance of NIPSA Intrusion Classification results.

The result shows that the overall accuracy rate was 99.42%, 98.27%, 97.40%, 97.40% and 96.54% based on the number of clusters used (4, 5, 6, 7, and 8, respectively). Moreover, it was identified that while the number of clusters increased beyond the number of data types, accuracy, precision, recall, and f-measure decreased while the false positive and false negative rates increased. Interestingly, the best result was generated when 4 clusters were used. Hence, the

proposed NIPSA intrusion classification performed best with 4 clusters. Table 1 shows the simple k-means clustering results of this paper.

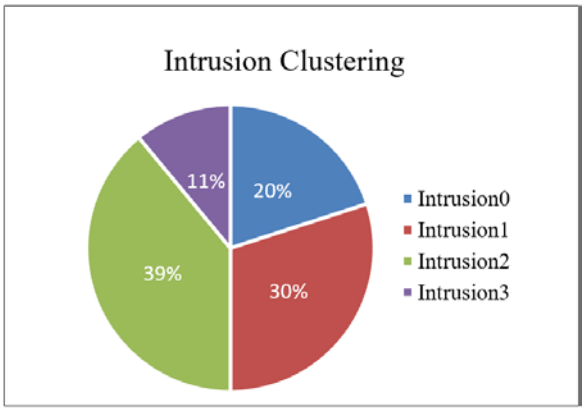

Fig. 7. Intrusion clustering.

Table 1. Simple k-means clustering results.

k	NIPSA Results (%)						
	TPR	**OA**	**FPR**	**FNR**	**Pr.**	**Rc.**	**F-1**
k = 4	99.4	99.42	0.3	0.6	99.4	99.4	99.4
k = 5	98.3	98.27	0.4	1.7	98.3	98.3	98.2
k = 6	97.4	97.40	0.7	2.6	97.5	97.4	97.4
k = 7	97.4	97.40	0.6	2.6	97.5	97.4	97.4
k = 8	96.5	96.54	0.8	3.5	96.6	96.5	96.5

6. Conclusion

In this paper, a new intrusion classification concept was developed based on research and testing performed in a laboratory. The performance of any intrusion detection and prevention system depends on its features and updated classification method of intrusion. The classification of intrusion was divided into five main categories: (i) infection (ii) propagation (iii) activation (iv) payload and (v) operating method. The developed conceptual intrusion classification will help implement the Network Based Intrusion Detection and Prevention System for better performance in future. Using the proposed intrusion classification, the experimental results indicate that the proposed NIPSA intrusion classification can identify intrusion with an overall rate of accuracy of 99.42%, a 0.3% FP rate, and a 0.6% FN rate. Efforts to develop more security techniques will continue in the future to further improve the efficiency of network intrusion classification.

References

1. Karatas, G.; and Sahingoz, O.K. (2018). Neural network based intrusion detection systems with different training functions. 6th *International Symposium on Digital Forensic and Security* (*ISDFS*). Antalya, Turkey, 1-6.
2. Ali, M.N.B. (2019). *A new model for network-based intrusion prevention system inspired by apoptosis*. Ph.D Thesis. Universiti Sains Islam Malaysia.

3. Mazini, M.; Shirazi, B.; and Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University-Computer and Information Sciences*, 31(4), 541-553.
4. Chad, P. (2008). The CIA triad. Retrieved September 21, 2018, from https://www.techrepublic.com/blog/it-security/the-cia-triad/
5. Rashmi, B.H. (2018). A strategical transition from information security to cyber security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 3(5), 700-704.
6. Deepika, B.; Vinod, S.; and Joshi, D.N. (2018). Current security project over hadoop and future perspective. *International Journal of Computer Engineering and Applications*, XII, Special Issue, 1-10.
7. McAfee (2018). McAfee labs threat report. Retrieved October 14, 2019, from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-dec-2018.pdf
8. Kayacik, H.G.; and Zincir-Heywood, A.N. (2009). Current challenges in intrusion detection systems. *Encyclopedia of Multimedia Technology and Networking*, Second Edition. Hershey, PA: Information Science Reference.
9. Rishi, V. (2019). Cyber security breaches survey 2019. Retrieved April 3, 2019, from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.
10. Ebenezer, P.; and Aderemi, A. (2017). Efficient feature selection technique for network intrusion detection system using discrete differential evolution and decision tree. *International Journal of Network Security*, 19(5), 660-669.
11. Paulauskas, N.; and Garsva, E. (2006). Computer system attack classification. *Electronics and Electrical Engineering, T*125 *Automation, Robotics*, 66(2), 1-4.
12. Howard, J.D. (1997). *An analysis of security incidents on the internet*, 1989-1995. PhD thesis. Carnegie Mellon University, Department of Engineering and Public Policy.
13. Salvatore, J.S.; Wei, F.; and Wenke, L. (2018). Cost-based modeling for fraud and intrusion detection: Results from the JAM project. Retrieved October 2, 2018, from https://kdd.ics.uci.edu/databases/kddcup99/task.html.
14. Kumar, S. (1995). *Classification and detection of computer Intrusions.* PhD thesis. West Lafayette, IN: Purdue University, Computer Sciences.
15. Saudi, M.M.; Tamil, E.M.; Cullen, A.J.; Woodward, M.E.; and Idris, M.Y.I. (2008). *Advance in Electrical engineering and computational science.* Chapter: Reverse engineering: EDOWA worm analysis and classification. Springer, 277-288.
16. Khaleel, A.; Verma, S.; Kumar, N.; and Shekhar, J. (2011). Classification of internet security attacks. *Proceedings of the* 5^{th} *National Conference; INDIACom.* Paschim Vihar, New Delhi, 229-230.
17. Ali, M.N.B.; Saudi, M.M.; Bhuiyan, T.; and Bakar, A.A. (2018). Comparative study of traditional and next generation IPS. *International Journal of Engineering and Technology*, 7(4), 55-58.
18. Aslam, S.; Ullah, S.; Siddique, M.A. and Sattar, A. (2017). Active attacks detection mechanism using 3-phase strategy. *IJCSNS International Journal of Computer Science and Network Security*, 17(1), 130-136.

19. Harshitha, B.; and Ramesh, N. (2013). A Survey of different types of Network Security threats and its countermeasures. *International Journal of Advanced Computational Engineering and Networking*, 1(6), 28-31.
20. Burns, D.; and Adesina, O. (2011). CCNP security IPS 642-627 official cert guide: network IPS traffic analysis methods, evasion possibilities, and anti-evasive countermeasures. Retrieved July 18, 2011, from http://www. Ciscopress.com/articles/article.asp?p=1728833&seqNum=3
21. Rouksana, S. (2017). Hackers are using encryption to bypass your security controls. Retrieved December 2019, from https://blogs.cisco.com/security/hackers-are-using-encryption-to-bypass-your-security-controls.
22. Ali, M.N.; Saudi, M.M.; Bhuiyan, T.; and Bakar, A.A. (2018). Comparative study of traditional and next generation IPS. *International Journal of Engineering and Technology*, 7(4.15), 55-58.