Detection and Defense Algorithms of Different Types of DDoS Attacks

Mohd Azahari Mohd Yusof, Fakariah Hani Mohd Ali, and Mohamad Yusof Darus

***Abstract*—Nowadays, computer network is very important because of the many advantages it has. However, it is also vulnerable to a lot of threats from attackers and the most common of such attack is the Distributed Denial of Service (DDoS) attack. This paper presents an overview of the existing detection and defense algorithms to mitigate four types of DDoS attacks and they are the UDP flood, TCP SYN flood, Ping of Death and Smurf attack. A detection and defense algorithm will be proposed in this paper and it will be evaluated using the existing Intrusion Detection and Prevention tool to determine whether it is the best algorithm to mitigate the DDoS attacks on a network environment. The proposed algorithm will be measured in terms of false positive rates and detection accuracy.**

***Index Terms*—DDoS, detection and defense algorithm, UDP flood, TCP SYN flood, ping of death and Smurf attack.**

I. Introduction

Nowadays, network and data are vulnerable to network attacks which may include DDoS attacks launched by attackers around the world to disrupt the network environment. According to [1], DDoS attacks are categorized as the most popular network attack because the attacks are most common around the world. Moreover, DDoS attack is easy to implement because its attack method is simple yet difficult to defense.

There are several types of DDoS attacks such as UDP flood, TCP SYN flood, Ping of Death, Smurf attack, DNS amplification attacks, HTTP flood and Slowloris [2].

II. Types of DDoS Attacks and ITS Effects

The basic of a DDoS attack is shown in Fig. 1, where an attacker uses several Zombies to make the attack stronger on the victims.

According to [3], there are three categories of DDoS attacks: volume-based attack, protocol attack and application layer attack.

Volume-based attack will flood the bandwidth of the attacked site and it is measured in bits per second. This kind of attack includes UDP flood, ICMP flood and other spoofed-packet flood. The protocol attack on the other hand will interrupt actual server resources and it is measured in packets per second. This includes TCP SYN flood, fragmented packet attack, Ping of Death and Smurf attack. The last is the application layer attack where it will crash the web server and it is measured in requests per second. This kind of attacks include Slowloris, Zero-day attack and DDoS attack that target Apache or Windows vulnerabilities.

This paper only focuses on four types of DDoS attacks: UDP flood, TCP SYN flood, Ping of Death and Smurf attack. These four types of DDoS attacks are common and very popular network attack launched by attackers [3]. In addition, it is easy to implement because its attack method is simple, but difficult to defense [4], [5]. Even though much research has been carried out to detect and defense different types of DDoS attacks throughout the world, still new methods of detection and defense task [6] need to be investigated in combating the never ending attacks on the network as technology changes very rapidly and so does the network attack .

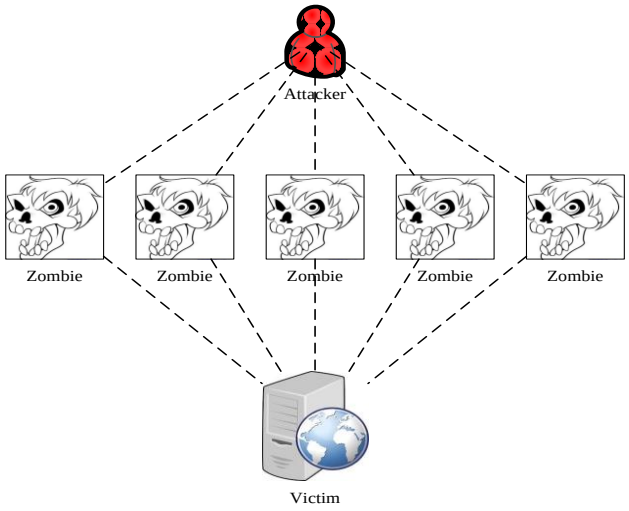

Fig. 1. Basic of DDoS attacks.

A. UDP Flood

UDP is a connectionless protocol in which there is no connection established before data transmission between the sender and receiver. In addition, UDP cannot detect the packet loss during the data transmission and it cannot send any error message. The biggest advantage of UDP compared to TCP is its high transmission speed. However, UDP packets can be exploited by attackers to launch UDP flood attacks such as high bandwidth attacks. UDP flood is launched by sending a large number of UDP packets to random destination ports to the victim's computer and this will slow

Manuscript received July 15, 2016; revised November 28, 2016.

Mohd Azahari Mohd Yusof is with Faculty of Computing and Technological Science, Kolej Universiti Poly-Tech MARA Kuala Lumpur, Malaysia (e-mail: azaha_ri@yahoo.com).

Fakariah Hani Mohd Ali and Mohamad Yusof Darus are with Faculty of Computer & Mathematical Sciences, Universiti Teknologi MARA Shah Alam, Malaysia (e-mail: fakariah@tmsk.uitm.edu.my, yusof@tmsk.uitm.edu.my.)

DOI: 10.7763/IJET.2017.V9.1008

down the computer system and crashes it [7] as shown in Fig. 2.

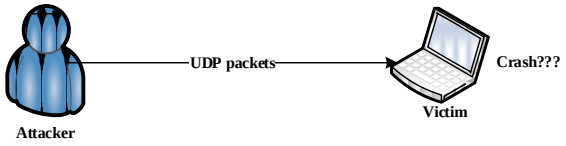

Fig. 2. UDP Flood attack.

B. TCP SYN Flood

In the TCP connection, client and server connection should be established first before data transmission. This is called TCP three-way handshake. The client needs to send SYN message to the server, then the server will acknowledge this by sending SYN-ACK message to the client and the client needs to send ACK message to the server and the connection is established. However, the normal TCP three-way handshake will turn into a TCP SYN flood when the attacker sends repeated SYN packets to random port on the targeted server by using a fake IP address [8] as shown in Fig. 3. The server will face some problems such as difficulty in closing the connection (connection stays open) and always receive a large number of SYN packets and yet no response is made to legitimate the clients and this can crash the server.

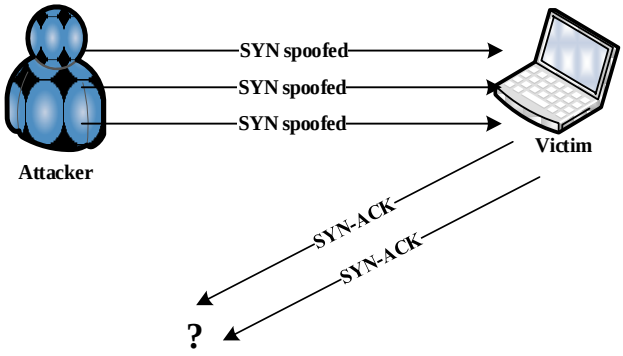

Fig. 3. TCP SYN Flood attack.

C. Ping of Death

The maximum size of the IP packet is 65535 bytes including the headers. The computer systems were never produced to handle a ping packet larger than the maximum packet size because it can violate the IP. Normally, the attackers send malformed packets in fragments. The fragment will be reassembled by the target system, but the packet is oversized and this will make the memory overflows and lead to various system problems, including crashes [9] as shown in Fig. 4. Ping of Death can be considered as an effective attack because the attacker's detail can be easily spoofed. Moreover, the attacker will need no detailed knowledge of the victim's computer except its IP address to launch the Ping of Death attack.

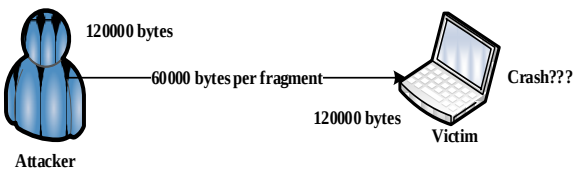

Fig. 4. Ping of Death attack.

D. Smurf

Smurf attack is launched by sending a large number of ICMP packets to the victim's computer and the computer system is flooded with spoofed ping messages [10] as shown in Fig. 5. There are five steps involved in launching a successful Smurf attack. The impact of a successful Smurf attack among others are crippled company server which may last for hours or days, lost revenue, customer frustration and theft of files or other intellectual property. Many Smurf attacks come bundled with rockets that allow attackers to create a backdoor for easy system access and it can take down a server or site of a company even if the attacker launches the attack using only little ping traffic.

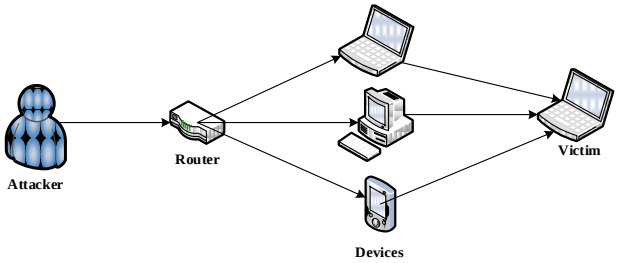

Fig. 5. Smurf attack.

E. Current DDoS Detection And Defense Algorithms

DDoS attacks are very prevalent and relatively easy to execute to interrupt a network environment. This is the reason why organizations need to have a way to detect and defense against DDoS attacks. There are several current algorithms designed to detect and defense different types of DDoS attacks.

The study conducted by [11] presents the design and implementation of an Artificial Immune System based on Dendritic Cell Algorithm. The system was used to detect DDoS attack and response to the detection activity to its generator. However, the algorithm is only used for TCP SYN flood attack detection.

The study conducted by [10] on the other hand focuses on the design of the ICMP traceback based on the Packet Marking Algorithm to identify DDoS attack. There are two evaluation methods used. The first method uses a virtual machine to implement the trackback system. The second method uses a simulation to evaluate the number of packets required to identify the attackers, who launched the attack. The algorithm is only used for Smurf attack detection.

The study by [12] looks at the traceback system by applying Packet Marking Algorithm to detect and prevent DDoS attack and identify the attacker's host information, even if they use spoofed IP address. The researchers test and evaluate the trackback system in terms of number of packets, time of processing for reconstruction and number of attack sources. Similar to the previous study, this algorithm is only used for TCP SYN flood attack detection.

Meanwhile a study conducted by [13] focuses on Packet Marking Algorithm to filter DDoS attack that contained fingerprint to identify attack packets coming from various sources even in case of IP spoofing. The researchers use the OMNET++ simulator to determine the algorithm can identify the attacker path mark and can mitigate the risks of TCP SYN

flood attack. This algorithm is only used for TCP SYN flood attack detection.

Another study conducted by [14] observes the Canny Edge Detector Algorithm as a model to detect DDoS attack by observing false positives, false alarm time, detection rate and detection delay. Again, this algorithm is only used for TCP SYN flood attack detection.

A study focuses on the dynamic changing security level strategy algorithm to protect neighboring nodes that are under attack and it can specify the type of attack was conducted by [15]. However, the algorithm is only used for TCP SYN flood attack detection.

The study conducted by [16] focuses on Rank Correlation Based Detection Algorithm to prevent web servers from DDoS attack. The algorithm is only used for TCP SYN flood attack detection.

The study conducted by [17] focuses on Worldwide SYN Flooding Attack Detection Algorithm to detect DDoS attack by using Netflow data and the algorithm is only used for TCP SYN flood attack detection.

The algorithms designed thus far are aimed at only detecting and defensing against TCP SYN flood, whilst there other types of attacks such as Ping of Death, Smurf attack, DNS amplification attack, HTTP flood and Slowloris that need to be detected.

III. Research Methodology Framework

There are seven phases in conducting this research as outlined in Fig. 6.

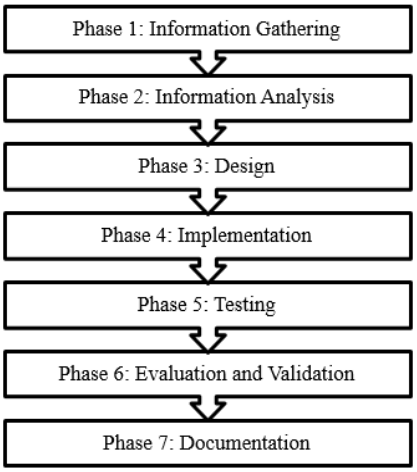

Fig. 6. Research methodology framework.

The first phase is Information Gathering, where it is used to find out literature related to the definition of DDoS attacks, types of DDoS attacks, how the DDoS attacks work and to study the behavior of DDoS attacks when the network is under attack. The second phase is Information Analysis, where it is used to find out several current DDoS detection and prevention algorithms, then study them and select the appropriate algorithms based on some selection criteria. The third phase is Design, where it is used to design DDoS detection and defense algorithms to detect and defense against UDP flood, TCP SYN flood, Ping of Death and Smurf attacks and propose a report of attacks to log specific information about the DDoS attack detected. The fourth phase is Implementation, where it is used to implement the proposed algorithms by executing the proposed algorithms to detect and create a defend system against UDP flood, TCP SYN flood, Ping of Death and Smurf attack. The fifth phase is Testing, where it used to test the proposed algorithms to measure the proposed algorithms in terms of false positive rates and detection accuracy. The sixth phase is Evaluation and Validation, where the experimental result is presented in a particular chart. The seventh phase is Documentation, where the research will be documented in a particular thesis format.

IV. Proposed Algorithms

This study will focus on designing a new DDoS detection and defense algorithms to mitigate UDP flood, TCP SYN flood, Ping of Death and Smurf attack. In the proposed algorithm, it focuses on three important parts: detection, defense and report of attacks as shown in Fig. 7.

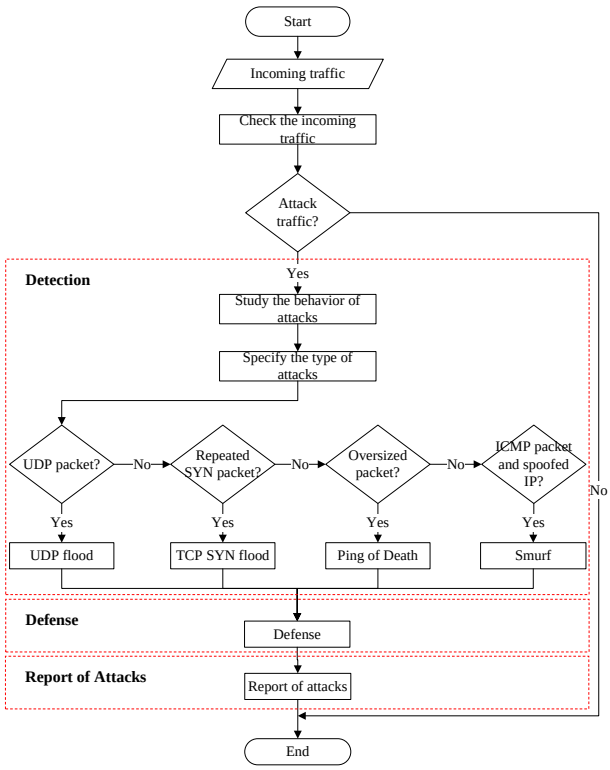

Fig. 7. Proposed design.

A. Detection

DDoS detection is very essential to the network environment to detect DDoS attacks because the attack is extremely easy to execute. The proposed detection algorithm is shown in Fig. 8.

The proposed detection algorithm will check the incoming traffic, whether it is DDoS traffic or normal traffic. If the incoming traffic is DDoS traffic, the proposed detection algorithm will specify the types of DDoS attacks, whether it is UDP flood, TCP SYN flood, Ping of Death or Smurf attack based on behavior of the attack.

B. Defense

The second part is defense, where it is used to block UDP flood, TCP SYN flood, Ping of Death and Smurf attack

before it reaches to the network as shown in Fig. 9.

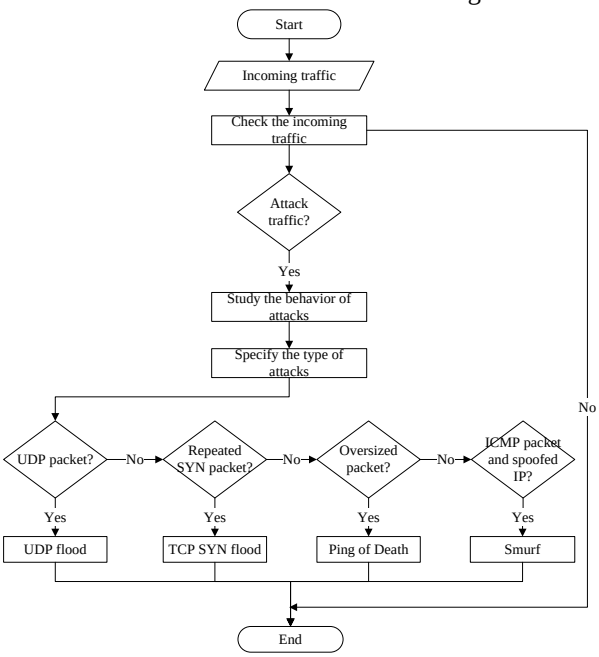

Fig. 8. Process of detection.

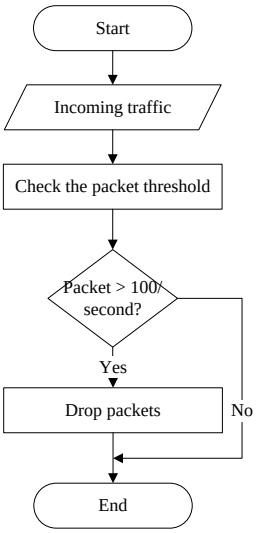

Fig. 9. Process of defense.

If the number of packets received is larger than 100 packets/second, the packet will be dropped automatically by the proposed defense algorithm. The hybrid of Snort and IPTables are used as full deep packet inspection, reduce the speed of incoming packets and control the use of network bandwidth. The proposed defense algorithm will ensure only clean traffic can penetrate into the network. The biggest strength of this defense algorithm is that protects the network even if a DDoS attack has been detected.

C. Report of Attacks

The report of attacks is very essential where it is used to log the types of DDoS attacks detected as shown in Fig. 10.

The strength of the report of attacks is produced continuously in real-time visibility into unwanted traffic and it will have the following details of the attack:

1) Types of DDoS attacks – There are four types of DDoS attacks: UDP flood, TCP SYN flood, Ping of Death and Smurf attack.
2) Packet size – Specifies the packet size, either random-sized or oversized of packet.
3) Severity level – Risk of attack, either it is low, medium or high level.
4) Detection time – Duration of the attacks flood the network.
5) Attacker source – The address that the packet was sent from the attacker, either it is using a real IP address or spoofed IP address.

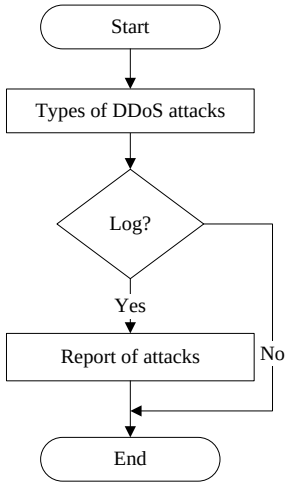

Fig. 10. Process of report of attacks.

V. Experimental Design

The experimental design of the proposed algorithm to be tested practically as shown in Fig. 11.

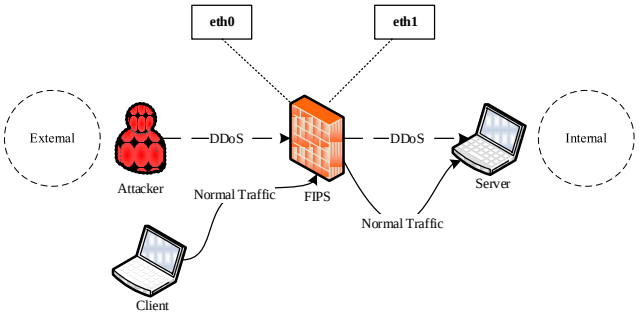

Fig. 11. Experimental setup.

In this experimental setup, four types of DDoS attacks: UDP flood, TCP SYN flood, Ping of Death and Smurf attack need to be generated by applying Putty Terminal for Windows and Terminal-based Wireshark (TShark). Firewall and hybrid of Snort and IPTables (FIPS) are required in order to implement and test the proposed algorithms injected into FIPS as a rule-based detection towards incoming packets. The proposed algorithms will specify the types of DDoS attacks, whether it is UDP flood, TCP SYN flood, Ping of Death or Smurf attack based on the behavior of attacks. Then, the hybrid of Snort and IPTables will function to drop the packet automatically before the attack reaches to the network infrastructure.

The proposed algorithms will be measured in terms of false positive rates and detection accuracy. According to [18], false positive rates is a normal or clean traffic incorrectly identified as an attack, while the detection accuracy is an ability of identifier to detect an attack with higher accuracy value for getting better detection results [19].

VI. Conclusion and Future Work

This paper reviewed four types of DDoS attacks and their effects and also several current DDoS detection and defense algorithm. The proposed detection and defense algorithm will be evaluated using the existing Intrusion Detection and Prevention tool to determine whether it is the best algorithm to mitigate the DDoS attacks towards a network environment. This research will then proceed with the implementation of the proposed algorithm to measure false positive rates and detection accuracy.

References

[1] McAfee Labs, "McAfee labs threats report," *McAfee*, Santa Clara, 2015.

[2] T. Reagor. 12 types of DDoS attacks used by hackers. [Online]. Available: http://www.rivalhost.com

[3] Imperva, "The top 10 DDoS attack trends," *Imperva*, California, 2015.

[4] Neustar, "The danger deepens: Neustar's annual DDoS attacks and impact report," pp. 1-14, 2014.

[5] S. Sivabalan and Radcliffe, "A novel framework to detect and block DDoS attack at the application layer," in *Porc. IEEE TENCON Spring Conference*, 2013, pp. 578-582.

[6] B. Rawal, H. Ramcharan, and A. Tsetse, "Emergence of DDoS resistant augmented split architecture," *IEEE High Capacity Optical Networks and Emerging/Enabling Technologies*, pp. 37-43, 2013.

[7] S. S. Kolahi, K. Treseangrat and B. Sarrafpour, "Analysis of UDP DDoS flood cyber attack and defense mechanisms on web server with Linux Ubuntu 13," in *Porc. International Conference on Communications, Signal Processing, and their Applications (ICCSPA)*, 2015, pp. 1-5.

[8] K. Geetha and N. Sreenath, "SYN flooding attack — Identification and analysis," *International Conference on Information Communication & Embedded Systems*, pp. 1-7, 2014.

[9] M. Buvaneswari and T. Subha, "IHONEYCOL: A distributed collaborative approach for mitigation of DDoS attack," *International Conference on Information Communication and Embedded Systems (ICICES)*, pp. 340-345.

[10] H. Guerid, A. Serhrouchni, M. Achemlal and K. Mittig, "A novel traceback approach for direct and reflected ICMP attacks," *IEEE Conference on Network and Information Systems Security (SAR-SSI)*, pp. 1-5, 2011.

[11] N. B. I. Al-Dabagh and I. A. Ali, "Design and implementation of artificial immune system for detecting flooding attacks," *International Conference on High Performance Computing and Simulation (HPCS)*, pp. 381-390, 2011.

[12] M. Vijayalakshmi, D. S. M. Shalinie and A. A. Pragash, "IP traceback system for network and application layer attacks," *IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 439-444, 2012.

[13] S. Saurabh and A. S. Sairam, "Linear and remainder packet marking for fast IP traceback," *IEEE Fourth International Conference on Communication Systems and Networks (COMSNETS 2012)*, pp. 1-8, 2012.

[14] C. James and H. A. Murthy, "Decoupling non-stationary and stationary components in long range network time series in the context of anomaly detection," *IEEE 37th Conference on Local Computer Networks (LCN),*, pp. 76-84, 2012.

[15] S.-H. Lim and J.-H. Kim, "Dynamic security level changing strategy using attack predictions-Case study of TCP SYN attacks," *IEEE International Conference on IT Convergence and Security (ICITCS)*, pp. 1-4, 2014.

[16] P. M. Priya, V. Akilandeswari, S. M. Shalinie, V. Lavanya, and M. S. Priya, "The Protocol Independent Detection and Classification (PIDC) system for DRDoS attack," *International Conference on Recent Trends in Information Technology*, pp. 1-7, 2014.

[17] L. Miao, W. Ding, and J. Gong, "A real-time method for detecting internet-wide SYN flooding attacks," *IEEE The 21st IEEE International Workshop on Local and Metropolitan Area Networks*, pp. 1-6, 2015.

[18] Trinita, Y. Purwanto, and T. W. Purboyo, "A sliding window technique for covariance matrix to detect anomalies on stream traffic," in *Porc. International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, pp. 176-181, 2015.

[19] M. I. W. Pramana, Y. Purwanto, and F. Y. Suratman, "DDoS detection using modified K-Means clustering with chain initialization over landmark window," in *Porc. International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, pp. 7-11, 2015.

Mohd Azahari Mohd Yusof received his bachelor in computer science (hons.) from University College of Technology & Management Malaysia (KUTPM) in 2006 and received his master of computer science (internetworking technology) from Universiti Teknikal Malaysia Melaka (UTeM) in 2013.

He is currently pursuing PhD degree in computer science at Universiti Teknologi MARA (UiTM), Malaysia. He has 10 years of teaching experience for undergraduate level. His current research interest is network security which focuses on the security towards network environment against different types of DDoS attacks.

Fakariah Hani Mohd Ali received her BSc (Hons) in information technology from Universiti Teknologi MARA (UiTM), Malaysia in 1999, a MSc in networking from Universiti Putra Malaysia (UPM) in 2004 and PhD of Security in Computing from Universiti Putra Malaysia (UPM) in 2009.

She is a senior lecturer at Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA (UiTM), Malaysia. She is a member of the Malaysian Society Cryptology Research (MSCR). Her current research interests include cryptography, digital forensics and network security.

Mohamad Yusof Darus received his bachelor in computer science from Universiti Teknologi Malaysia (UTM) in 1999, a master of information technology from Universiti Utara Malaysia (UUM) in 2003 and PhD degree in Computer Science from Universiti Teknologi Malaysia (UTM) in 2013.

In 2003, he joined the Department of Computer Technology & Networking, Faculty of Computer and Mathematical Scienes, Universiti Teknologi MARA (UiTM), Malaysia. His current research interests include wireless network, computer security and VANETs.