# Attack Intention Recognition: A Review

Abdulghani Ali Ahmed, Noorul Ahlami Kamarul Zaman
*(Corresponding author: Abdulghani Ali Ahmed)*

Faculty of Computer Systems & Software Engineering, Universiti Malaysia Pahang
26300 Gambang, Pahang, Malaysia
(Email: abdulghani@ump.edu.my)

*(Received Nov. 3, 2015; revised and accepted Apr. 6 & May 7, 2016)*

## Abstract

Sensitive information faces critical risks when it is transmitted through computer networks. Existing protection systems are still limited in their capacities to ensure network information has sufficient confidentiality, integrity, and availability. The rapid development in network technologies has only helped increase network attacks and hide their malicious intent. This paper analyzes attack types and classifies them according to their intent. A causal network approach is used to recognize attackers' plans and predict their intentions. Attack intention is the ultimate attack goal which the attacker attempts to achieve by executing various methods or techniques, and recognizing it will help security administrators select an appropriate protection system.

*Keywords: Attack intention recognition, causal network approach, cyber security, network forensics*

## 1 Introduction

Information security over a network has become more challenging due to the expansion of technologies for hacking and anti-forensics. Sensitive information should be treated confidentially in any system as it represents a high risk to the owners if exposed to the public. Information is at risk due to several factors, including human and technical errors, accidents and disasters, fraud, commercial espionage, and malicious damage [1, 2, 4].

Activities such as unauthorized access, damage to computer data or programs, obstruction of the functions of computer systems or networks, interception of data, and computer espionage are categorized as cybercrimes [7, 8, 10, 11, 17, 21]. Cybercrimes are broad in scope and are defined as attacks that involve the use of computers or networks to commit the crimes. According to [3, 4, 9], cyber-attacks can be categorized into unauthorized access, malicious code (malware), and interruption of services. Figure 1 shows common types of network threats.

Network forensics, as a part of network security, works with laws and guiding principles established in the judicial system to deal with cyber criminals. Network forensics has two approaches: reactive and proactive. Reactive network forensics is a traditional approach that deals with cybercrime cases a period of time after an attack. The reactive forensic approach consumes considerable time during the investigation phase. Proactive network forensics is a new, different approach that focuses on investigating concurrently with an attack [5, 14].

Figure 2 shows a framework of the generic process model in network forensics that splits the phases into two groups. The first group relies on actual time and includes five phases: preparation, detection, incident response, collection, and preservation. The second group relies on the post-investigation phases.

Authors in [16] also classify the first group as proactive and the second group as reactive. The proactive phases have advantages in saving time and money during investigation, as they work concurrently with the occurrence of the cybercrime. By contrast, reactive phases begin with the examination phase to integrate the trace data and identify the attack indicators. The indicators are then prepared for the analysis phase, which reconstructs the attack indicators either by soft computing or statistical or data mining techniques to classify and correlate the attack patterns. Attack intention is the ultimate goal the attacker is attempting to achieve by executing various methods or techniques of attack. Even for an expert, it is difficult to predict methods of attack. An attacker will work toward his goal through a sequence of tactical steps using sophisticated techniques to hide and cover his patterns. Attack Intention Recognition (AIR) is the process of using known attack scenarios to observe an attacker's behavior and infer his intention [19]. With the rapid developments in networking technology, attacks have become more dangerous than ever, deploying sophisticated mechanisms to hide malicious behavior. Understanding attackers' behavior will help security administrators recognize their intentions and better predict their activities.

In the following section, work related to this research is critically analyzed. This study discusses using proactive AIR methods to identify attack plans to predict future ac-

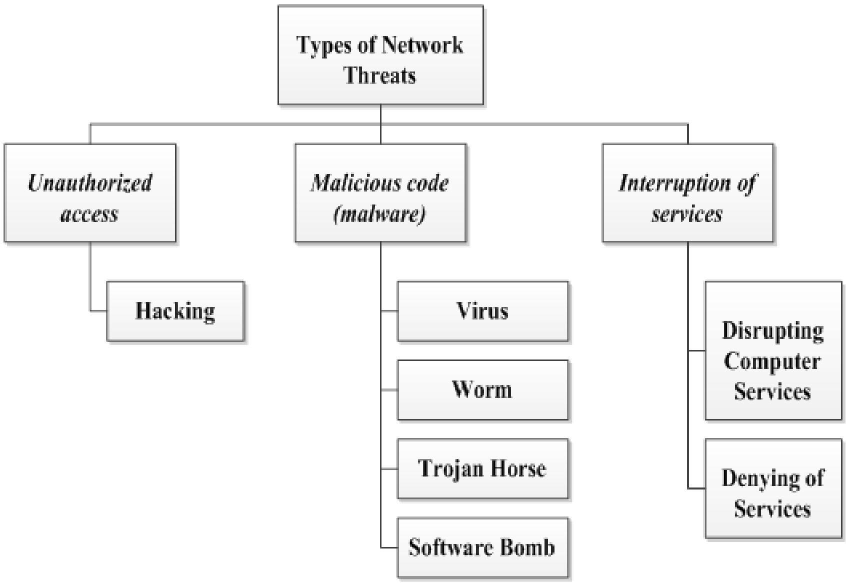


Figure 1: Common types of network threats

tions. The remainder of the paper is organized as follows. Section 2 reviews related works. Section 3 critically discusses the most relevant works, and Section 4 concludes this paper.

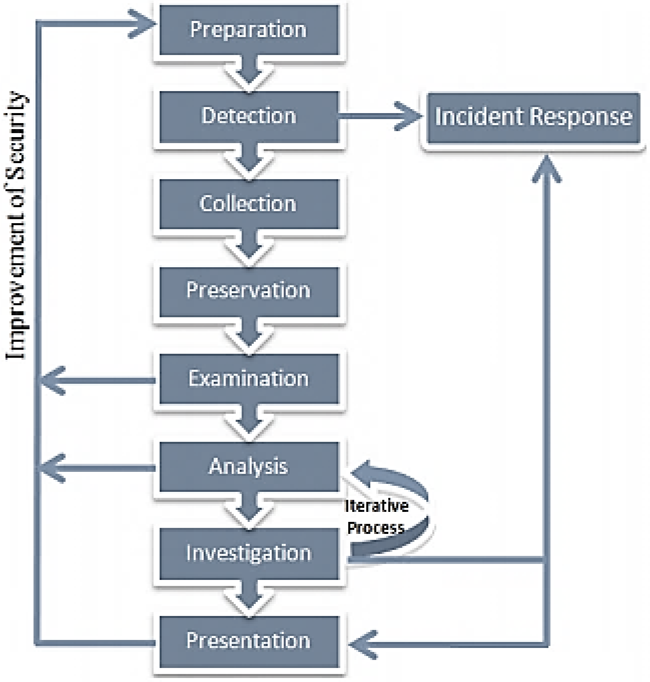


Figure 2: Generic process model

## 2 Related Works

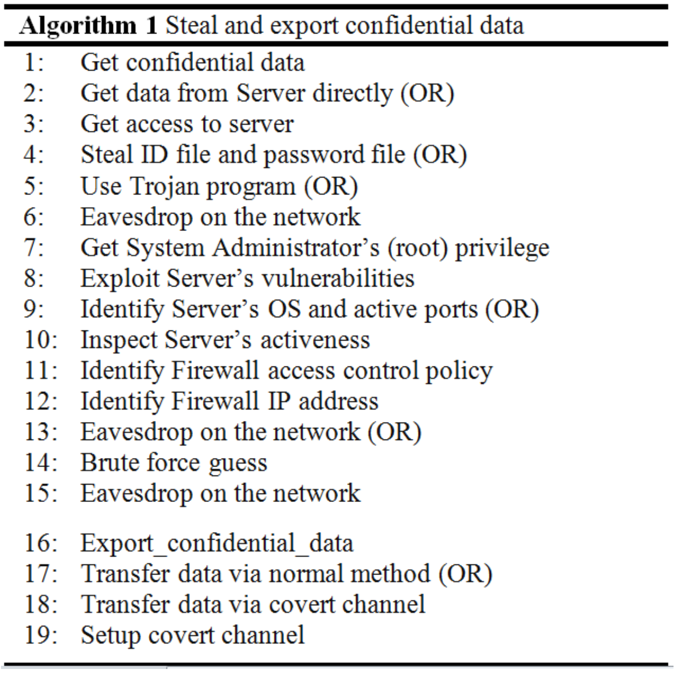
Numerous studies have studied different approaches to AIR and its various methods of implementation [13, 14, 15, 18, 19, 20]. The approaches that focus on identifying attack intention are causal networks, path analysis, graphical attack, and Dynamic Bayesian Network (DBN). These approaches are described with further detail in the following subsection.

### 2.1 Causal Networks

The researchers in [12] studied security alert correlation, which focuses on conducting probabilistic inference to correlate and analyze attack scenarios. From the analysis, they attempted to solve other issues: (1) to identify attacker's tactics and intention and (2) to predict potential attacks. Recognizing attack plans is the process of deducing the aims of an attack from observations of its activities. Alert correlation analysis is significant for avoiding potential attacks and minimizing damage. To explicate all paths through a system which an intruder may use to accomplish his goal, attack plans or libraries are used, usually denoted by graphs. The security or vulnerability of a system is then computed by an attack tree analysis, which is based on the attacker's aims. This type of analysis can be used as a baseline for threat detection, defense, and response. However, it is a manual and time consuming process and is less scalable for a large network.

An example of an attack tree of methods for stealing and externally exporting data stored on a server is shown in Algorithm 1. The sample indicates that to obtain confidential data, an attacker may use several methods such as downloading data directly from the server or eavesdropping on the network. To gain access to a server, it is necessary to acquire normal users' or system administrators' privileges (root).

To correlate isolated alerts, attack trees are adopted to define attack plan libraries. They are then converted to causal networks so that probability distribution can be assigned. The benefit to defining attack tree nodes by attack classes rather than specific attack is the reduced complexity of the computation for the probabilistic inference on the causal network. In implementation, a directed acyclic graph illustrates a causal network (Bayesian network), where each node symbolizes a variable with a certain set of states and directed edges denoting the cause of the dependent relationship among the variables. Probabilistic inference is applied to the causal network to evaluate goals by reviewing attack activities, thereby predicting potential future attacks.



**Algorithm 1** Steal and export confidential data

```
Get confidential data
Get data from Server directly (OR)
Get access to server
Steal ID file and password file (OR)
Use Trojan program (OR)
Eavesdrop on the network
Get System Administrator's (root) privilege
Exploit Server's vulnerabilities
Identify Server's OS and active ports (OR)
Inspect Server's activeness
Identify Firewall access control policy
Identify Firewall IP address
Eavesdrop on the network (OR)
Brute force guess
Eavesdrop on the network

Export_confidential_data
Transfer data via normal method (OR)
Transfer data via covert channel
Setup covert channel
```

For the test, any scenarios that have similar end goals are grouped under one evidence set due to correlated aims. This method applies attack trees to the library of attack plans. From the results observed, attack scenarios automatically correlate isolated attacks and ensure network security is controlled.

Based on [13, 15], attack intention analysis is a predictive factor for facilitating the accurate investigation of a case. This paper proposed a technique combining Dempster-Shafer (D-S) evidence theory with a probabilistic method through a causal network to predict attack intentions. The purpose of this research is to support decision making by selecting and predicting actual attack intentions and determining the best response, regardless of feasibility.

The experiment results show that the accuracy of prediction is related to the amount of evidence collected. The results also show that security can determine the highest priority value among intention probability values and make a decision that minimizes the use of time and money. However, this research has limitations. Identifying the attack intention is difficult if the malicious action is distinct from predefined attack classes. Distinguishing a deception from actual aims of attackers is also challenging. Another challenge is determining whether there is a single attacker or a collaborative group.

## 2.2 Path Analysis

The researchers in [18] proposed a technique that uses attack path analysis and can provide protective measures at minimum cost. Knowing an attacker's intention can help network guards make decisions as they can more easily predict potential attack paths and evaluate threats. When an attack scenario recognizes an intruder's intention, it is detailed by an attack path. Usually, successful attacks comprise a series of vulnerability exploits that grant the privileges of the projected host and use them to attack the final target. To determine the attack path on a network, the attack path on a victim host should be specified. Figure 3 shows possible attack scenarios. Note that multiple vulnerabilities can be exploited to achieve the same goal. Each attack path starts from the access node (local node) and ends at the higher privilege node.

A complete set of the possible attack paths on a victim host can be calculated using a path finding algorithm. The algorithm uses vulnerabilities, privileges, and host information to produce a graph of the attack path. A graph comprising all possible attack paths is computed once a model of the network configuration and the victim host are input. In this paper, it is assumed that an attacker will not cover his tracks after reaching his target. Generating an attack path graph requires the parameters of the host, privileges, intention, output of attack paths on a victim host on the network, and information on the network configuration.

For each network, intentions can be determined based on either the vulnerabilities and topology of the network or the focus of its business. Attention is then given to larger probability intentions. This study proposes assessing the threat by recognizing an attacker's intention and predicting the attack path. By applying the Bayesian rule, the threat situation of the entire network can be calculated when the intentions are known.

To reach the network guards' goal of protective measures at minimum cost, the minimum number of nodes is cut. Thus, an intrusive intention can be determined from the initial point using an attack path graph, which is a directed acyclic graph, to evaluate intention threat. In the experiment, intention probabilities can be computed based on the degree of difficulty in exploiting vulnerabilities. An intention capable of greater damage represents a larger value of consequence. To ensure security of the network, all intentions of attack should be blocked.

Conversely, given that attack paths remove the minimum number of nodes to disconnect the intrusive inten-

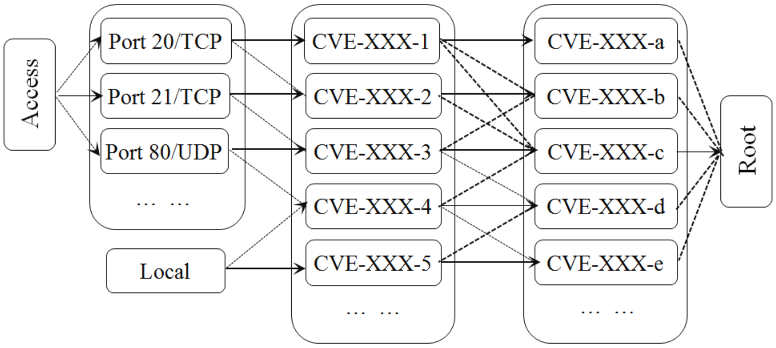


Figure 3: Framework of attack path on victim host

tion from the initial point, there is a probability that the removed nodes themselves are the target of attack. In such cases, the attack intention can go unrecognized.

### 2.3 Graphical Attack

The graphical model in [19] was used to recognize attack intention. The researchers attempted to verify the feasibility and validity of this method. A network security states graph, which is a directed graph, was used as a graphical model of attacks. In this model, the said graph is represented by nodes of security states that include both the states of the system and the attacker. The edges of the graph denote a relationship of state transition under the actions of attackers. No circuit is present in the graph as it is presumed that the attacker will not re-intrude a host he has attacked. There is a pseudocode of algorithm that generates a network security states graph. This pseudocode shows the initial state of the network and uses available attack actions as input. To infer uncertain intentions, D-S evidence theory is used. A threat assessment is presented to evaluate the security level of a network based on the situation and the value of the intended target is determined. Figure 4 illustrates an example of a security states graph. Every "S" node is a state of network. The "H" links are hosts, and "a"s are exploitations of vulnerabilities.

Similar to the previous technique, this method also assumes that attackers have several attack plans to achieve the same intention. With D-S evidence theory, possibly every attack plan can be derived. It is useful for providing evidence and guiding decision making. The authors in [6] define attack graphs as an instrument that works out the hierarchical steps of an attack scenario by using vulnerabilities and configuration. Thus, the type attack, whether normal or anti-forensics, can be identified. Anti-forensics, as described in this paper, uses methods such as deleting system logs after hacking into a computer to prevent tracking by authorities. Using the attack evidence graph, the existence of anti-forensics attacks can be determined. The tools and techniques used by the attacker can also be identified. However, with the current mechanisms used in anti-forensics, system configuration and vulnerability information are not enough to trace the path. This is because security depends on vulnerability data but attackers use anti-forensics to hinder this action. Moreover, this approach only aims to identify the intention of the unauthorized access to a network or host that an attacker may compromise. Thus, attackers with privileged access to network are an identified challenge in this approach.

### 2.4 Dynamic Bayesian Network

As discussed in [20], the Dynamic Bayesian Networks (DBN) method is proposed for identifying intrusion intention. This research aims to improve on the limitation of current Intrusion Detection System (IDS) technology, which fails to apply a logical relationship between attack events. DBN is a technique for combining a static Bayesian network and a timestamp to form a new probabilistic model from the removal of order data. Figure 5 shows the DBN based on the intrusion intention identification model: (a) prior network, (b) transfer network, and (c) DBN model in time.

For the scenarios, given that a large aggregation of training data are available, the Markova Assumption is used to assume the attack goal, depending only on intentions observed under restrictions plus the last completed goal and the latest attack behavior. The process in reaching the final attack goal, based on intrusion alarm messages, is shown in Figure 6.

The experiment assumes the goal with the most probability is the final attack goal of the intruder. In this process, the final target is identified when the attacker compromises another target first to gain privilege. The disadvantage of this approach is its dependency on the last completed goal and latest attack behavior.

## 3 Related Work Analysis and Discussion

This section compares the related works and analyzes their models. From the discussion above, it may be

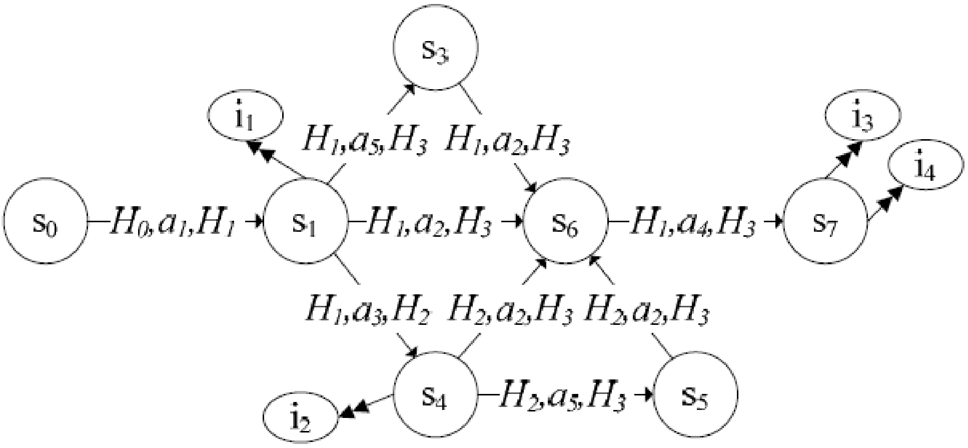


Figure 4: Example of security states graph

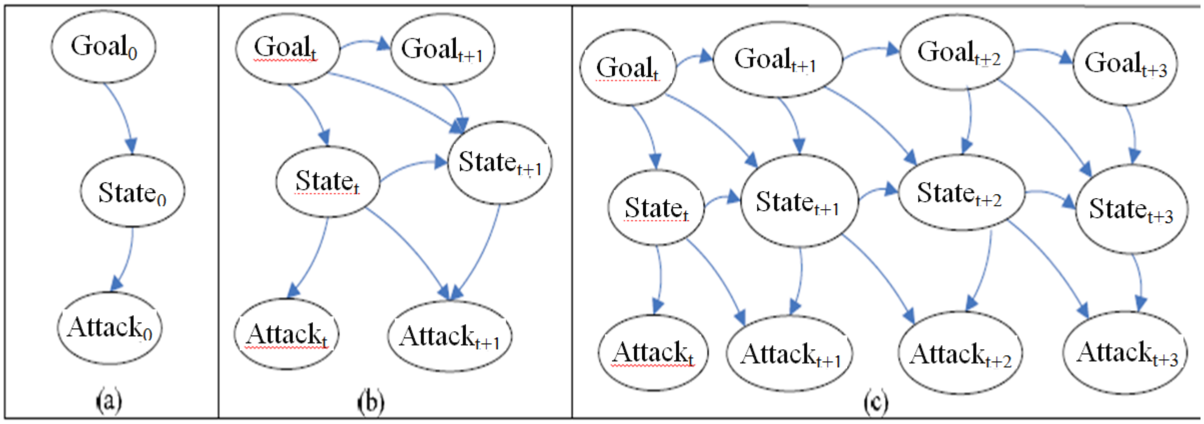


Figure 5: Dynamic Bayesian network architecture

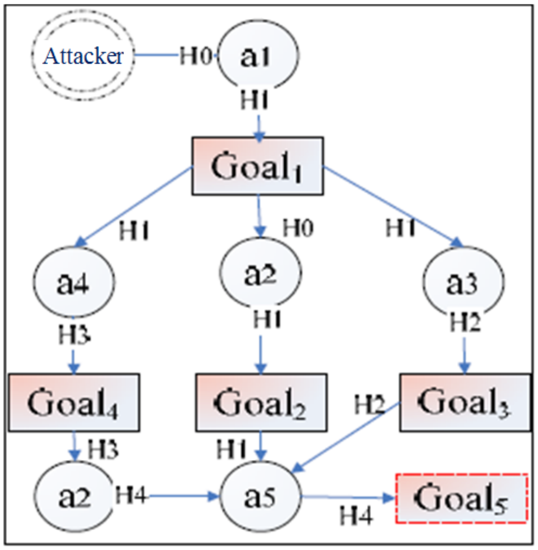


Figure 6: Process of reaching the final attack goal

observed that there are similar methods used in different models such as D-S evidence theory, Bayesian rule, and directed acyclic graphs. D-S evidence theory focuses on uncertainty to conclude the intention of an attack [22]. Bayesian rule applies probabilistic reasoning for threat assessment or determining the goal of the intrusion. Directed acyclic graphs track attacks. Directed acyclic graphs track attacks using several methods such as attack path, attack tree, or attack plan. However, attack trees have some drawbacks. They are manual processes, time consuming, and are limited to the attack plans in the library [12]. That said, the library can be expanded through the participation of security experts. Besides competence in attack recognition, the other advantages of the aforementioned approaches are discussed. Graphical models use network security states graphs. The algorithm proposed infers intent and conducts threat assessment. Similar to the graphical approach, causal networks also use graph-based techniques to correlate isolated attack scenarios after observing their relationships in attack plans. It is proposed for pinpointing attack plans and predicting upcoming attacks. However, causal networks have an added value: by applying probabilistic inference to evaluate the likelihood of attack goals and forecast upcoming attacks based on causal networks converted from attack trees. An attack path analysis model approach to constructing attack path graphs can also recognize the intrusive intention and simultaneously calculate the threat of intention. This approach can find protective measures at minimum cost with the theory of minimum cut. Moreover, a DBN adopts probabilistic reasoning for estimating an attack. This technique can identify the intrusion intention with various alarm messages and predict incoming attacks in real-time. That said, each of the aforementioned approaches has certain limitations. These limitations are summarized in Table 1.

Table 1: Disadvantages of attack intention recognition models

| Model | Limitations |
|---|---|
| Causal network | • If malicious actions are different from the predefined scope of attack, it is hard to identify them.<br>• It is difficult to distinguish deception and actual plans of attackers.<br>• It is difficult to determine whether the actual number of attackers. |
| Attack path | • Only presents the first step toward identifying intrusive intention. |
| Graphical | • Only presents the first step toward identifying intrusive intention. |
| Dynamic Bayesian networks | • Given that the attack assumption is based on the latest action, it will not work in a case of uncertain attack. |

Although attack path analysis, graphical model, and causal network approaches all apply graphs in their methods, causal networks have another added value in that they compare attack path analyses and graphical models. Besides providing graph-based techniques to correlate isolated attack scenarios, they apply probabilistic inference to evaluate the likelihood of attack goals and forecast upcoming attacks based on causal networks converted from attack trees. Thus, the causal network approach will be adopted to solve the problems in this research.

## 4 Conclusion

This paper reviews various approaches toward attack intention recognition, including causal networks, path analysis, graphical attack, and DBNs with Markova assumptions. These approaches are all interrelated, differing from each other due to the aims of researchers. Basing on the review performed on the existing works and the critical analysis of their advantages and disadvantages, we conclude that using a causal network approach is effective for detecting network attacks that have similar intentions. For future study, an experiment will be performed to evaluate the efficiency of detecting an attack's intention. This can entail testing various methods for detecting attack intentions and seeing how each method performs in a true lab environment under real world scenarios.

## Acknowledgments

RDU grant number RDU1403162, Faculty of Computer System & Software Engineering, Universiti Malaysia Pahang supported this work.

## References

[1] A. A. Ahmed, A. Jantan, and M. Rasmi, "Service violation monitoring model for detecting and tracing bandwidth abuse," *Journal of Network and Systems Management*, vol. 21, no. 2, pp. 218–237, 2013.

[2] A. A. Ahmed, A. Jantan, and T. C. Wan, "Sla-based complementary approach for network intrusion detection," *Computer Communications*, vol. 34, no. 14, pp. 1738–1749, 2011.

[3] A. A. Ahmed, A. Jantan, and T. C. Wan, "Real-time detection of intrusive traffic in qos network domains," *IEEE Security & Privacy*, vol. 11, no. 6, pp. 45–53, 2013.

[4] A. A. Ahmed, A. Jantan, and T. C. Wan, "Filtration model for the detection of malicious traffic in large-scale networks," *Computer Communications*, vol. 82, no. 59-70, pp. 15–23, 2015.

[5] A. A. Ahmed, A. S. Sadiq, and M. F. Zolkipli, "Traceback model for identifying sources of distributed attacks in real time," *Security and Communication Networks*, 2016.

[6] R. Chandran and W. Q. Yan, "A comprehensive survey of antiforensics for network security," *Managing Trust in Cyberspace*, pp. 419–447, 2013.

[7] T. W. Che, J. F. Ma, Na Li, and C. Wang, "A security quantitative analysis method for access control based on security entropy," *International Journal of Network Security*, vol. 17, no. 5, pp. 517–521, 2015.

[8] B. B. Gupta, R. C. Joshi, and M. Misra, "Ann based scheme to predict number of zombies in a ddos attack.," *International Journal of Network Security*, vol. 14, no. 2, pp. 61–70, 2012.

[9] M. S. Hwang and C. C. Lee, "Research issues and challenges for multiple digital signatures.," *International Journal of Network Security*, vol. 1, no. 1, pp. 1–7, 2005.

[10] C. C. Lee, M. S. Hwang, and I-En Liao, "On the security of self-certified public keys," *International Journal of Information Security and Privacy*, vol. 5, no. 2, pp. 55–62, 2011.

[11] C. C. Lee, C. H. Liu, and M. S. Hwang, "Guessing attacks on strong-password authentication protocol.," *International Journal of Network Security*, vol. 15, no. 1, pp. 64–67, 2013.

[12] X. Qin and W. Lee, "Attack plan recognition and prediction using causal networks," in *20th IEEE Annual Computer Security Applications Conference*, pp. 370–379, 2004.

[13] M. Rasmi and A. Jantan, "Aia: Attack intention analysis algorithm based on D-S theory with causal technique for network forensics- a case study," *International Journal of Digital Content Technology and its Applications*, vol. 5, no. 9, pp. 230–237, 2011.

[14] M. Rasmi and A. Al-Qerem, "Pnfea: A proposal approach for proactive network forensics evidence analysis to resolve cyber crimes," *International Journal of Computer Network and Information Security*, vol. 7, no. 2, pp. 1–25, 2015.

[15] M. Rasmi and A. Jantan, "Attack intention analysis model for network forensics," in *Software Engineering and Computer Systems*, vol. 2, pp. 403–411, Springer, 2011.

[16] M. Rasmi, A. Jantan, and H. Al-Mimi, "A new approach for resolving cyber crime in network forensics based on generic process model," in *The 6th International Conference on Information Technology (ICIT'13)*, pp. 45–53, 2013.

[17] S. Saurabh and A. S. Sairam, "Increasing accuracy and reliability of ip traceback for ddos attack using completion condition," *International Journal of Network Security*, vol. 18, no. 2, pp. 224–234, 2016.

[18] P. Wu, Y. Shuping, and J. Chen, "Recognizing intrusive intention and assessing threat based on attack path analysis," in *IEEE International Conference on Multimedia Information Networking and Security (MINES'09)*, vol. 2, pp. 450–453, 2009.

[19] P. Wu, Z. Wang, and J. Chen, "Research on attack intention recognition based on graphical model," in *Fifth IEEE International Conference on Information Assurance and Security (IAS'09)*, vol. 1, pp. 360–363, 2009.

[20] Q. Wu, R. Zheng, G. Li, and J. Zhang, "Intrusion intention identification methods based on dynamic bayesian networks," *Procedia Engineering*, vol. 15, pp. 3433–3438, 2011.

[21] Z. Yunos, R. Ahmad, and N. A. M. Sabri, "A qualitative analysis for evaluating a cyber terrorism framework in malaysia," *Information Security Journal: A Global Perspective*, vol. 24, no. 1-3, pp. 15–23, 2015.

[22] Y. Zhang, L. Yu, and W. Li, "Research of ds evidence method in network attack intention recognition," in *2nd International Conference on Electronic & Mechanical Engineering and Information Technology*, pp. 2325–2328, Atlantis Press, 2012.

**Abdulghani Ali Ahmed** biography. Abdulghani Ali Ahmed is a senior lecturer in the Faculty of Computer Systems & Software Engineering at Universiti Malaysia Pahang. His research interests include information security, digital forensic and cybercrimes investigation, MPLS technology, QoS and embedded real-time systems. Ahmed received the PhD in network security from Universiti Sains Malaysia in 2014. He is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the International Association of Engineers (IAENG). Contact him at abdulghani@ump.edu.my.

**Noorul Ahlami Kamarul Zaman** biography. Noorul Ahlami Kamarul Zaman received the Bachelor in computer systems & networking with honors from University Malaysia Pahang in 2014. She received the Master in computer networking from University Malaysia Pahang in 2016. Her area of interest includes cyber security and network forensics.