AIRSE: An Approach for Attack Intention Recognition Based on Similarity of Evidences

Abdulghani Ali Ahmed*, Noorul Ahlami Kamarul Zaman
Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang, 26300, Kuantan, Pahang, Malaysia
abdulghani@ump.edu.my, noorul.ahlami@gmail.com

Abstract. Sensitive information can be exposed to critical risks when communicated through computer networks. The ability of attackers in hiding their attacks' intention obstructs existing protection systems to early prevent their attacks and avoid any possible sabotage in network systems. In this paper, we propose a similarity approach called **A**ttack **I**ntention **R**ecognition based on **S**imilarity of **E**vidences (*AIRSE*). In particular, the proposed approach *AIRSE* aims to recognize attack intention in real time. It classifies attacks according to their characteristics and uses the similar metric method to identify attacks motives and predict their intentions. In this study, attack intentions are categorized into specific and general intentions. General intentions are recognized by investigating violations against the security metrics of confidentiality, integrity, availability, and authenticity. Specific intentions are recognized by investigating the network attacks used to achieve a violation. The obtained results demonstrate that the proposed approach is capable of investigating similarity of attack signatures and recognizing the intentions of network attack.

Keywords: Cyberattacks, Network forensics, Attack intention recognition, Similarity of evidences

1 Introduction

With the rapid advancement of networking technologies, attacks become more dangerous as attackers utilize more advanced methods to hide their intentions. Identifying the motives of attackers allows security administrators to predict and counter attack intention which is the ultimate reason why an attack was conducted. In general, it is difficult to predict the attack intentions as the attackers use a set of tactical steps supported by techniques to hide and cover their malicious activities [1].

* Abdulghani Ali Ahmed
Faculty of Computer Systems & Software Engineering
Universiti Malaysia Pahang
abdulghani@ump.edu.my

The intention of an attack is what the attack hopes to achieve. Recognizing hostile intentions helps security administrators develop security systems to thwart attackers with certain motives. Attack intention recognition (AIR) is the process of using known attack scenarios to observe an attacker's behavior and infer his intention [2]. 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.

There are few approaches in the attack intention recognition that have been studied in many research papers with different ways of implementation. Authors in [2] classify these approaches into causal network [1], path analysis [3], attack graph [4], dynamic bayesian network [5], attack intention analysis algorithm [6], and similarity intention metric [7]. Although helpful, these approaches still have several problems that may critically affect th e efficiency and capability of recognizing the attack intentions in real time,

This study proposes a similarity approach called **A**ttack **I**ntention **R**ecognition based on **S**imilarity of **E**vidences (*AIRSE*). In particular, *AIRSE* approach is proposed to recognize attack intention in real time based on investigating the similarity of attack characteristics through two main stages. A pattern of attack is created as a baseline for intention recognition in the first stage. In the second stage, the attack intention then is recognized by investigating the similarity between the characteristics of the created pattern and the evidence collected from a detected attack. The rest of this paper is organized as follows. Section 2 is the literature review. Section 3 proposes *AIRSE* approach. *AIRSE* implementation is described in Section 4. Section 5 discusses the results of this study. Section 6 concludes this paper.

2 Related Works

Multiple researches have studied different approaches to AIR and its various methods of implementation. In [2], the approaches of AIR are categorized into causal networks, path analysis, graphical model, and dynamic Bayesian network, intention analysis, and similarity intention metric as illustrated in Fig. 1. The following subsections describe the different approaches of AIR with further detail.

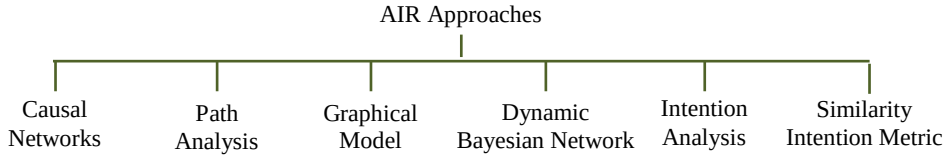

Fig. 1. AIR approaches

Causal network was presented by [1] to identify and predict possible attacks. This study developed a graph-based technique to correlate isolated attacks using low-level alerts and comparison to known attack plans. Probabilistic interference was used to evaluate the probabilities of an attack having certain goals to create causal network attack trees for attack prediction. This study uses predefined attack plans created with expert inputs to predict and thwart possible attacks. If attack' activities are beyond the scope of existing attack plans, the creation of new attack plans is required. The creation of mechanisms to identify the true and apparent motives of attackers is also necessary, as well as tools to distinguish single attackers and multiple attackers.

Attack path analysis was proposed in [3] and involves the use of graphical attack paths to predict attacker motives. In attack path analysis, intrusive intensions and the threat the pose can be quantified. Minimum cut theory is used to identify the minimum necessary resources to accomplish objectives. This study is only the first step in identifying and addressing threats, although several possible options for future research appear promising, such as the use of additional parameters to improve accuracy or the quantification of the time and money needed to use certain methods.

Graphical models, as proposed by [4], are used to recognise attacker motives. The state of network security is represented by the use of nodes to represent both the defending system and the attackers. Changes in system defenses are represented graphically as the attack occurs. The method assumes that the attackers have one goal and multiple attack plans. Attack graphs can be used to map out the steps of an attack scenario using known vulnerabilities and configurations, as stated by [8]. Graphical models effectiveness is limited to unauthorised network access and does not cover attacks made using privileged access.

Dynamic bayesian networks (DBN) are a tool for identifying intrusion first proposed by [5]. DBN combines static bayesian networks with timestamps to order remove data using a probabilistic model in order to identify attacker motives. DBN uses Markova assumptions and large amounts of training data with the latest attack behaviors and objectives to identify attacker intensions. This study assumes that the most probable attack goal is the true goal of an attacker and that attacker's compromise multiple targets to gain the necessary resources to complete their objectives.

Based on [6], attack intention analysis is a predictor used to accurately facilitate securities. This study proposes a technique combining mathematical Dempster-Shafer (D-S) evidence theory with a probabilistic method in a causal network to predict attacker intentions. Prediction accuracy is related to the amount of collected evidences. This approach needs to have a library of potential intentions and evidence to quickly determine true intentions.

A Similarity of Attack Intentions (SAI) algorithm was proposed by [7] as an improvement to Attack Intention Analysis (AIA). It forms similar intentions between a new attack and previous attacks by estimating the similarity values between the new and old attack intentions. SAI uses cosine similarity as a distance-based similarity measure to estimate similar cybercrime intentions. The maximum similar attack intention value is selected to identify the similarities between the intention of the new attack and previous

attacks. This method selects the closest match to the intentions of the new attack as the real intentions of the attack. Table 1 summarizes the limitations of the reviewed approaches.

Table 1. Disadvantages of attack intention recognition approaches

Model	Disadvantage
Causal network	- If malicious actions else from the predefined scope of attack, hard to identify them. - Problem in distinguishing the deceptive plan and real aim of attackers - Difficulty in differentiating the number of attackers, whether a single attacker or collaborated group.
Path analysis	- Only present first step in identifying intrusive intention.
Graphical Model	- Only present first step in identifying intrusive intention.
Dynamic Bayesian networks	- Since the attack assumption is based on latest action, will not work on uncertain attack.
Attack intention analysis	- Need to have library of intentions in order to determine the true intentions early.
Similarity intention metric	- Still need to apply AIA algorithm.

3 Proposed Approach AIRSE

Fig. 2 illustrates the architecture of the proposed approach *AIRSE*. In particular, *AIRSE* recognizes attack intention using two main phases. First, the pattern of attack is created as a baseline for intention recognition. Second, the attack intention is recognized by investigating the similarity between the signatures of the created pattern and the evidence collected from a particular attack. .

Pattern creation phase creates a baseline that is used to detect attack intentions. In this study, attack intentions are categorized into general and specific intentions. General intentions are recognized by investigating violations against the security metrics of confidentiality, integrity, availability, and authenticity. Specific intentions are recognized by investigating the different attacks used to achieve a violation. The recognized general and specific intentions are utilized as a baseline to recognize the intention of new attacks. The attack pattern is created by extracting the signatures of attacks and classified them in categories according to each attack. Intention recognition phase recognizes the main and specific intentions of network attacks by investigating the similarity between collected evidence and the classified signatures of network attacks. The similarity is investigated using formula (1) as stated in [7].

$$\mathrm{Sim}A_n E(A_k) = \mathrm{SumSimAE}(A_k) \,/\, r. \quad \textbf{(1)}$$

where $SimA_nE$ (A_k) is the similar attack evidence for each attack, SumSimAE (A_k) is summation of the similar attack evidence, and r is the total number of A_k evidence. The similarity values were calculated for each intention and sorted in descending order.

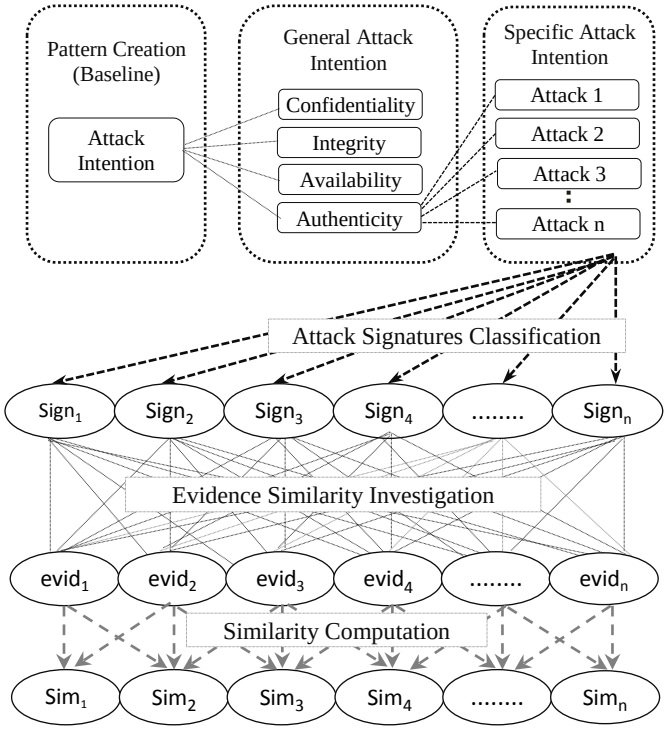

Fig. 2. AIRSE architecture

4 AIRSE Implementation

In this study, network attacks are classified into four categories based on their possible violations on the main parameters of information security [9-11] as shown in Table 2. This study limits attack threats to five categories as described in Table 3. Unlike [7], which use similarity of intention to recognize attack intention, this study uses the similarity of evidence features to discover real intention as shown in Table 4.

Table 2. Categories of attacks according to security parameters

Security Parameter	Type of Attacks
Confidentiality	Spoofing attack, sniffing attack, access attack
Integrity	Code execution, spoofing attack, malware
Availability	DoS, DDoS, botnet
Authenticity	Spoofing attack, brute force, malware

Table 3. Instances of network attacks

ID	Attack Type	Instance
A_1	DoS	SYN flooding, Ping of death, Smurf attack
A_2	DDoS	SYN flooding, Ping of death, Smurf attack
A_3	Botnet	Zombie army
A_4	Malware	Worm, Virus, Trojan horse
A_5	Spoofing attack	Man-in-the-Middle, DNS Spoofing

Table 4. Predefined attack evidences

ID	Evidence Type	Vulnerability
E_1	Source IP address	Single, Multiple
E_2	Destination IP address	Single, Multiple
E_3	Port number	21, 23, 25, 53, 80, 111
E_4	Time to live (TTL)	TTL expired
E_5	Protocol type	NTP, SMTP, FTP, HTTP
E_6	Packet size	65,536 bytes
E_7	Service type	Unknown port number or type of protocol
E_8	Operating system	CVE-2013-3899, CVE-2013-3195, CVE-2013-3940
E_9	Software	Open source, free
E_{10}	Host performance	Bandwidth, CPU, Memory, Kernel memory

Table 5 displays connections between types of attacks based on their vulnerabilities. Port numbers (E_3) have the greatest possibility to be targeted for attack, while TTL (E_4) is the least likely vulnerability to be targeted except by DoS (A_1). In addition, DDoS (A_2) is the most likely attack to be launched. *AIRSE's* algorithm shown in Fig. 3 is proposed to develop a proactive approach to improve attack intention recognition. This algorithm is a modification of the Similarity of Attack Intention (SAI) algorithm. In particular, it creates a solution from similarity of attack evidence to discover attack intentions. *AIRSE* evaluates evidences and attack features to recognize intention. Fig. 3 also illustrates how the intention similarity metric is generated from ($SimAE(A_k)$). The maximum evidence similarity metric is selected to identify the similarities between the evidence and the new

attack and previous attacks using (SimAE(A_k)). The closest match to the evidence of the new attack is used to discover real attack intentions.

Table 5. Attacks and their possible evidences

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}
A_1	x		x	x		x	x			x
A_2	x	x	x		x	x	x			x
A_3	x	x	x				x			x
A_4			x						x	x
A_5			x		x					

Input : Attack with their evidence probability.
Output : Estimate similar of the new attack intentions with other.
Begin
Let PA a set of predefined attacks {A_1,A_2,A_3…A_5}
Define A_k as a new attack, where A_k ϵ PA
Let AE a set of predefined attack evidence {e_1,e_2,e_3…e_{10}}
Define E_x as a set of all attack evidence for A_k, where E_x ϵ AE
Initialize the maximum similarity of attack evidence with A_k, MaxSimAE(A_k) = 0
Initialize the summation of all similarity of attack evidence with A_k, SumSimAE(A_k) = 0
For each A_n ϵ PA **do**
  For each E_m ϵ AE **do**
    Select E_d where E_d ϵ E_x
    If E_d founds, **then**
      Assign A_nE_d as the probability value of E_d
    Else
      Assign A_nE_d = 0
    End If
    Compute SumSimAE(A_k) = SumSimAE(A_k) + A_nE_d
  End For
  Compute SimA_nE(A_k) = SumSimAE(A_k) / r, as a similar attack evidence, where r is the total number of A_k evidences
  If SimA_nE(A_k) > MaxSimAE(A_k), **then**
    Assign MaxSimAE(A_k) = SimA_nE(A_k)
    Select n as an a maximum similar attack number
  End If
End For
End

Fig. 3. AIRSE algorithm

5 Results and Discussion

This section describes the results of *AIRSE* study. To allocate intention value, *AIRSE* implements [12] technique to specify the value of attack evidence based on importance and frequency of occurrence. It was decided that the minimum weight for attack evidence was 0, or no evidence found, and the maximum value was 1. The new attack A_6 evidence was analysed with priority and frequency weights, and four evidence sets were identified: $\{E_1, E_3, E_5, E_{10}\}$. The potential evidence for the new cybercrime are $\{E_3, E_5\}$ because they have the maximum probability value reserved for the E_x set where x represents the number of evidence sets as shown in Table 6. The value for evidence determines the accuracy of the height value for detection after the analysis process. Each value equals (0.70). The predefined attack set is PA = $\{A_1, A_2, A_3 \ldots A_5\}$, and the predefined evidence set is AE = $\{E_1, E_2, E_3 \ldots E_{10}\}$.

Table 6. Evidence probability values for all attacks

	E_1	E_2	E_3	E_4	E_5	E_6	E_7	E_8	E_9	E_{10}
A_1	0.79	0	0.75	0.59	0	0.45	0.56	0	0	0.78
A_2	0.68	0.72	0.81	0	0.5	0.55	0.7	0	0	0.88
A_3	0.5	0.63	0.78	0	0	0	0.58	0	0	0.9
A_4	0	0	0.2	0	0	0	0	0	0.63	0.88
A_5	0	0	0.9	0	0.7	0	0	0	0	0
A_6	0.43	0	0.7	0	0.7	0	0	0	0	0.21

Table 7 shows the similarity of evidences values between A_6 and the other predefined attacks. *AIRSE* algorithm identifies similar evidence $\{E_3, E_5\}$ between the new attack A_6 and predefined attacks. Among these attacks, A_6 is similar to a spoofing attack, and A_5 has the highest similarity value for all three comparisons. In conclusion, the general intention of the new attack A_6 is unauthorized access to network system (authenticity violation) and the specific intention the attacker used to achieve the unauthorized access is identity spoofing.

Table 7. The similar evidence values for E_3 and E_5

	Similarity with (E_3)	Similarity with (E_5)	Similarity with (E_3) & (E_5)
A_1	0.75	0	0.375
A_2	0.81	0.5	0.655
A_3	0.78	0	0.39
A_4	0	0.65	0.325
A_5	0.9	0.7	0.8

The obtained results demonstrate that the *AIRSE* algorithm increases the possibility of recognizing intentions in advance, allowing for the elimination of similar cases based on evidence similarity. The results shows the relationship between new attacks and predefined attacks to help in the decision making process. Table 8 shows a comparison between *AIRSE* and other existing approaches of attack intention recognition. The comparison process shows that *AIRSE* algorithm is an efficient approach for intention recognition.

Table 8. Comparison between AIRSE and other approaches

Criteria	AIRSE	SAI	Path analysis	Attack graph
Require predefined type of attack	Yes	Yes	Yes	Yes
Require predefined evidences	Yes	Yes	Yes	Yes
Require predefined intentions	No	Yes	Yes	Yes
Require attack plan library	No	No	Yes	Yes
Mode of operation	Auto	Auto	Auto	Manual
Need support from other methods	No	Yes	Yes	Yes
Number of attack can be catered	Unlimited	Unlimited	Limited	Limited
Rate of consistency	Medium	High	High	Low

6 Conclusion

This paper reviews several approaches of attack intention recognition and critically discusses their limitations. We proposed *AIRSE* approach in order to mitigate the limitations of the existing approach. The finding of this paper demonstrates that *AIRSE* provides useful information and increases the possibility of recognizing attack intentions in advance by eliminating similar cases using evidences similarity. The finding also demonstrates that usage of data gathered from previous invasions is beneficial for future attack predictions.

A limitation of this paper is associated with the implementation part. *AIRSE* was implemented using limited number of evidences as well as the weights allocated for attack features are uncertain. As recommendations for future research, deep analysis on the attacks features would provide more accurate values, allowing for multiple sets of evidence to reduce the time required in recognizing attack intention. This recommendation could be achieved using training behaviours for attack evidence to recognize attack intention using an Artificial Neural Network (ANN).

Acknowledgments

RDU grant number RDU160365, Faculty of Computer System and Software Engineering, Universiti Malaysia Pahang supported this work.

References

[1] Qin, Xinzhou, and Wenke Lee. "Attack plan recognition and prediction using causal networks." In Computer Security Applications Conference. 20th Annual, pp. 370-379. IEEE,(2004).

[2] Ahmed, Abdulghani Ali, and Noorul Ahlami Kamarul Zaman. "Attack Intention Recognition: A Review." International Journal of Network Security. 19, 244-250, (2017).

[3] Peng, Wu, Shuping Yao, and Junhua Chen. "Recognizing Intrusive Intention and Assessing Threat Based on Attack Path Analysis." In 2009 International Conference on Multimedia Information Networking and Security. vol. 2, pp. 450-453. IEEE (2009).

[4] Peng, Wu, Zhigang Wang, and Junhua Chen. "Research on attack intention recognition based on graphical model." In Information Assurance and Security, 2009. IAS'09. Fifth International Conference on. vol. 1, pp. 360-363. IEEE (2009).

[5] Wu, Qingtao, Ruijuan Zheng, Guanfeng Li, and Juwei Zhang. "Intrusion intention identification methods based on dynamic bayesian networks." Procedia Engineering 15, 3433- 3438, (2011).

[6] Rasmi, M., and Aman 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. 5, 230 - 237, (2011).

[7] Rasmi, Mohammad, and Aman Jantan. "A New Algorithm to Estimate the Similarity between the Intentions of the Cyber Crimes for Network Forensics." Procedia technology. 11, 540-547, (2013).

[8] Thampi, Sabu M., Bharat Bhargava, and Pradeep K. Atrey, eds. Managing Trust in Cyberspace. CRC Press, (2013).

[9] Sumra, Irshad Ahmed, Halabi Bin Hasbullah, and Jamalul-lail Bin AbManan. "Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey." In Vehicular Ad-Hoc Networks for Smart Cities, pp. 51-61. Springer Singapore, (2015).

[10] Ahmed, Abdulghani Ali, Aman Jantan, and Tat-Chee Wan. "Filtration model for the detection of malicious traffic in large-scale networks." Computer Communications. 82, 59-70, (2016).

[11] Ahmed, Abdulghani Ali, Ali Safa Sadiq, and Mohamad Fadli Zolkipli. "Traceback model for identifying sources of distributed attacks in real time." Security and Communication Networks (2016).

[12] Al-Utrakchi, E. A. and AL-Mousa, M. R. A new model for preanalysis of network traffic using similarity measurement. International Conference on Information Technology, 7: pp. 349-353, (2015).