國立交通大學

電機與控制工程學系

碩士論文

基於攻擊圖形的混合式無線網路風險評估方法

A Hybrid Approach for Attack Graph-Based Risk Assessment of Wireless Networks

研究生：鍾興龍

指導教授：黃育綸 博士

中華民國九十七年七月

基於攻擊圖形的混合式無線網路風險評估方法
A Hybrid Approach for Attack Graph-Based Risk Assessment of Wireless Networks

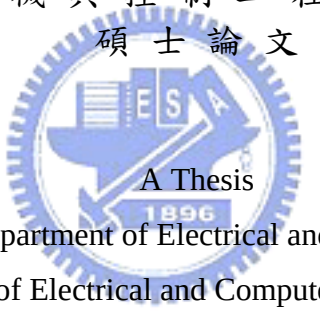
研 究 生：鍾興龍　　Student：Hsing-Lung Chung

指導教授：黃育綸 博士　　Advisor：Dr. Yu-Lun Huang

國 立 交 通 大 學

電 機 與 控 制 工 程 學 系

碩 士 論 文



A Thesis

Submitted to Department of Electrical and Control Engineering

College of Electrical and Computer Engineering

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Electrical and Control Engineering

July 2007

Hsinchu, Taiwan, Republic of China

中華民國九十七年七月

基於攻擊圖形的混合式無線網路風險評估方法

學生：鍾興龍　　指導教授：黃育綸 博士

國立交通大學電機與控制工程學系（研究所）碩士班

摘　　要

無線網路風險評估是無線安全領域中的關鍵技術之一。為了幫助管理者評估網路之安全程度，攻擊圖形以圖形化的表示方式來呈現分析結果，提供管理者在決策時的參考依據。近年來，許多學者利用層級程序分析法(Analytic Hierarchy Process Method，AHP)及模糊語意量測法(Fuzzy Linguistic Measure method)來處理風險評估的問題，其網路評估架構以 3 層為主，然而此架構並不能表示各種網路配置資訊對不同類型無線網路攻擊所造成的影響，再者，層級程序分析法適用在不隨環境變動的評估項與評估法則間建立判斷矩陣，對於會隨環境變動的評估項，其擴充性較差；模糊語意量測法較難從模糊集合中取得量化數值，無法提供精確的分析結果。因此，我們結合層級程序分析法及模糊語意量測法並加以改良，提出一套分析無線網路安全性的風險評估模型。在此模型中，我們定義了一個 4 階層的無線網路風險評估架構，從此架構中，我們透過分析法則來求得每個配置資訊在不同網路攻擊類型中的影響程度，並使用模糊權重平均法(Fuzzy Weight Average Method，FWA)來計算各攻擊類型的模糊平均集合；為了能夠取得各個攻擊類型數值化的風險等級，我們設計一個量化方法從模糊平均集合求得量化數值。之後便可結合層級程序分析法，以所定義的專家經驗為基礎來計算風險值。最後，我們利用兩個無線網路上常見的拓樸為範例，證明此風險評估模型的有效性與實用性並利用圖形化工具 Graphviz 產生攻擊圖形來描述其風險值。

A Hybrid Approach Attack Graph-Based Risk Assessment of Wireless Networks

Student: Hsing-Long Chung Advisor: Dr. Yu-Lun Huang

Department of Electrical and Control Engineering

National Chiao Tung University

Abstract

Risk assessment of wireless networks is one of the crucial techniques in the area of wireless network security. A graph-based representation, called attack graph, has been developed to appear analytic results and support policies for administrators. Recently, the analytic hierarchy process (AHP) method and the fuzzy linguistic measure method have been applied to deal with risk assessment problems. The assessment architecture is based on 3 layers. However, the architecture can not represent influence of configurations on different attack types. In addition, the AHP method is hardly constructed judge matrixes if analysis items changed with network environment while the fuzzy linguistic measure method is hardly acquire quantifiable value from fuzzy set. Hence, we modify and combine the two methods to establish a new risk assessment model to analyze the security robustness of wireless networks. In the proposed model, we redefine 4-layer assessment architecture of wireless networks. From this architecture, we can obtain influential level of each configuration on different attack types through analysis rules and use the fuzzy weight average (FWA) method to calculate average fuzzy set of each attack type. In order to gather quantitative risk rating of each attack type, a quantitative method is designed to obtain value of average fuzzy set. Afterward the AHP method is applied to compute the risk value based on expert experience. Finally, two case studies are given to demonstrate validity and feasibility for risk assessment according to the proposed model. We also use the Graphviz tool to generate their attack graphs to describe the security robustness of these two examples.

誌　　謝

兩年的碩士班求學過程，要感謝的人很多。特別要感謝指導教授黃育綸老師，兩年來細心的指導與關懷，除使得本論文得以順利完成之外，也讓我學習到做人做事的道理，使我受益良多，在此表示由衷的謝意。在研究的過程中，您不時的給予我在想法上的啟發，也在我遇到困難與挫折時，竭盡所能的給予我最大的幫助與鼓勵，並時時刻刻注意學生在研究上的進度，適度的給予糾正及調整研究的方向，使得我能夠有繼續研究的動力。同時，也要感謝謝續平教授、曾文貴教授、以及何福軒博士，在口試期間提出的寶貴意見與指正，使我可以了解論文不足的地方，並對此進行改善，使得本論文更加完整。

其次，感謝「即時嵌入式系統實驗室」的黃詠文學長以及蔡欣宜學姐在論文上的指導；也感謝其餘實驗室的成員在學業上的切磋，透過彼此間腦力激盪，使得我的觀念更加的清晰並啟發更多的想法，此外實驗室閒暇之餘的娛樂活動，讓我能夠在身心愉悅的情況下持續我的研究，增加我對實驗室的向心力；也感謝其他交大的師長、同學、朋友們，在學習道路上的指引與陪伴，透過彼此的專長來合力完成許多專案計畫，增加我在專案計畫上的經驗；感謝大學時期的同學，在生活及研究上給我的幫助，像是在研究上的經驗以及生活資訊的提供，使我獲益良多。

除此之外，特別要感謝辛苦扶養我長大的父親、母親，還有我的妹妹，不論是在生活上及精神上，都是我最重要的支柱，由於你們的關愛與支持，讓我無後顧之憂，也才有今天的我。

最後，向在我人生道路上，一路陪伴我走來的所有人們，獻上最誠摯的祝福與感謝。

Table of Contents

List of Tables

List of Figures

Chapter 1
Introduction

In today's society, wireless networks bring great convenience to network users, and also brings a large collection of threats into wireless environment. For this reason, a risk assessment model in design of wireless networks has become a popular issue in order to deal with security problems. Furthermore, the attack graph is proposed to display the results of risk assessment. The first chapter of this thesis is organized in to three sub sections: Section 1.1 presents the background of this research. Our contribution is presents in section 1.2, and the remainder of the thesis is introduced in section 1.3.

1.1 Background

Wireless networks have become the most interesting target for attackers because they use airwave instead of physical medium to interconnect wireless devices or stations. Several papers have published some specific threats to wireless networks. In [1], the researchers pointed out the weaknesses in WEP encryption. One of the main vulnerabilities in WEP is that the uses of a 32-bit CRC checksum and a 24-bit Initialization Vector (IV) for the encryption algorithm. The CRC checksum was intended to detect unintentional errors in the packet. Attackers could still modify the packet and calculate a new CRC checksum to make it look the unmodified. The problem with the 24-bit IVs was that the IVs were too few to guarantee only use at one time. Attackers will see enough traffic to completely exhaust the entire domain of the 24-bit IVs, and then they could see two encrypted packets with the same IVs to crack the encryption key. In addition, the RC4 algorithm had less security because of the weak key [2]. The problems of WEP have been improved by WPA, but Lehembre [3] mentioned the

most practical vulnerability was WPA's PSK key. The key could be obtained through dictionary attack. Some wireless attacks including eavesdropping attack, man in the middle attack, access attack, DoS attack and DDoS attack, were illustrated in [4]-[7]. Attackers will utilize some important information from wireless packets. From [4], Welch *et al.* presented the encrypted tunnels of network layer and data link layer as explained in Fig. 1. Hence attackers can identify the source and destination MAC address when layer 2 is employed. Layer 3 encryption let the IP address of sender and receiver open for viewing.

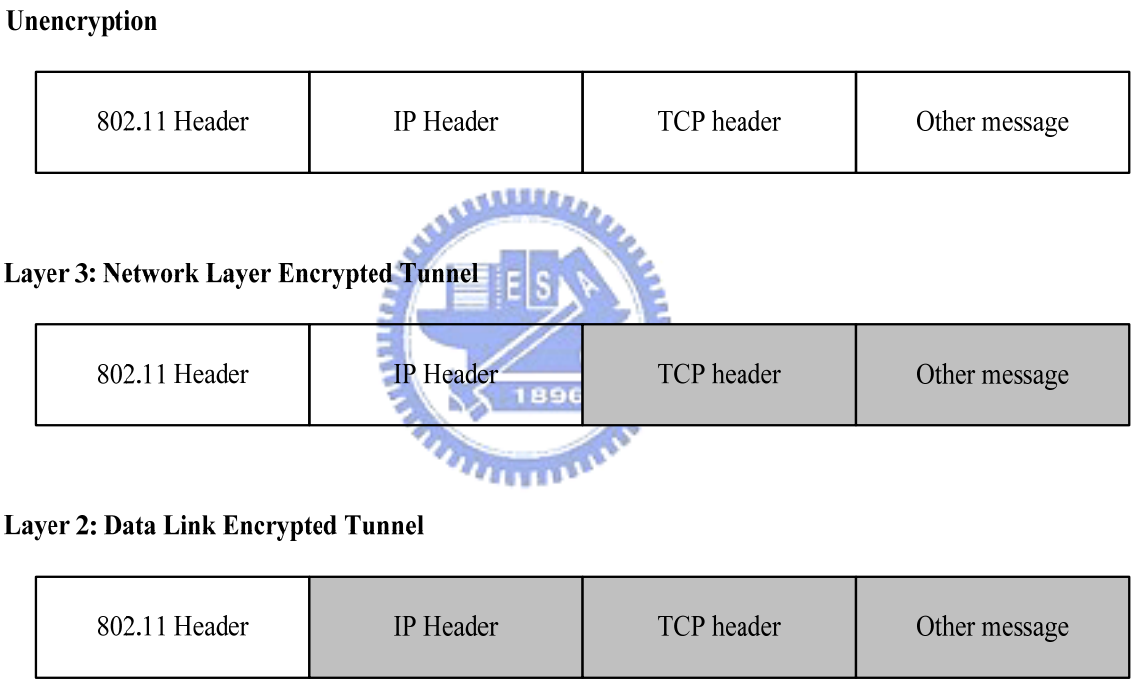


Fig. 1. Layer Encryption (Welch *et al.* [4])

Nowadays, administrators can use a lot of tools find the security holes of each host that may cause attacks. In order to defend attacks efficiently, a graphical environment is needed for security issues. Attack graph is a graphical representation and has focused on security analysis. At first it is used to appear the vulnerabilities of the host. As the development of network, the attack graph not only displays the vulnerabilities among the network, but also describes the attack behavior of attackers. After that some researchers use attack graph to

analyze the safety of the network environment according to the network configurations. Altogether, the arrack graph provides a view to help administrators understand where the security problems are and support them to make the environment more robust.

Attack graphs have traditionally been constructed manually by administrators [8]. But more recently, the network environment becomes more and more vast and complex. Constructing attack graphs by the hand is impractical and tedious. Thus, significant progress has been made to generate attack graph automatically [9]-[16].

The development of attack graph includes vulnerability description [9]-[16], risk assessment [17], reliability analysis [18] etc. The way to enhance the network security before being attacked is risk assessment.

The advantages of network security risk assessment are as follows: (1)Monitoring critical information and protecting the network environment more effectively;(2)Supporting the security policies quickly for decision maker;(3)Providing useful information for administrators [19]-[21].

There are several risk assessment methods, such as cause-consequence tree analysis and fault tree analysis, etc. The methods usually use mathematical or statistical techniques to evaluate risk values [22]. However, these methods are not suitable for wireless network security risk analysis because the security issues focus on environment of wireless networks. Recently, we know risk analysis can be analyzed through linguistics method or analytic hierarchy process (AHP) method, but there are some drawbacks of the two methods. These issues we will discuss later.

The purpose of this thesis is to establish an assessment model. The model contains an extendable assessment architecture and a risk analysis method for quantitative value of wireless network security. We then use tool to produce attack graph for wireless network analysis. The nodes and edges of attack graphs denote wireless device and risk value between two nodes, respectively. Hence administrators can easily understand the security robustness of

WLAN.

1.2 Contribution

A major advance of the assessment architecture in this thesis over other risk assessment architectures is that it considers the configurations of wireless networks. It is more flexible than the exiting architectures due to the fact that some configurations of each node will be changed at any moment by the users. Furthermore, the risk assessment method, which combines the AHP method and the linguistics of the fuzzy measure method, is applied to the risk assessment. The approaches can objectively determine the judge matrixes and the risk weight of risk factors based on the expert experiment. Afterward the total risk value can be calculated through matrix operation.

1.3 Synopsis

The rest of this thesis is organized as follow. In Chapter 2, we review related work in this area. In Chapter 3, we propose new hierarchical risk assessment architecture and risk analysis method for wireless network security. Chapter 4 gives 2 examples to illustrate the proposed architecture is useful to network risk assessment. In addition, we provide a view of attack graph based on the configurations of WLAN. Finally, Chapter 5 presents some conclusions.

Chapter 2

Related Work

Wireless networks have many security holes that may cause attacks and attackers always use these holes to achieve their goals. In order to keep attackers from accessing, monitoring and modifying network packets, some security tools can help to detect the configurations information of wireless networks. Furthermore, the administrators can use the configurations for risk assessment and show the risk value in the graph. These graphs collect the crucial information to aid network administrators in efficiently reinforcing network security. In this chapter, we first review the past researches for attack graph. Section 2.2 specifies the process of risk assessment. The risk assessment approaches of network are reviewed in section 2.3.

2.1 Past Researches for Attack Graph

Attack graphs have been widely used in security issues. Any attack or vulnerability could be observed from the path which went from an initial node to a success node. Formerly, the attack graph in which each node represented a state of attackers, and each edge represented an atomic attack that changed the state. Initial nodes expressed the states that attackers had not conducted any atomic attack, and success nodes expressed the states that attackers had successfully reached his goal [10]. Such the attack graph became very complex if the network added more hosts. As a result, an automatic tool is useful for administrators to establish the attack graph.

Many methods have been proposed to define the attack graph and automatically construct it. Ortalo *et al.* [9] developed a method named privilege graph, the nodes in privilege graph represented privileges owned by the users and the edges represented

vulnerabilities that would change privileges. The graph displayed different ways that attackers could reach his goal. From [10], Philips and Swiler defined an attack graph which was generated by three types of input: attack templates, configurations file, and attacker profiles. Attack templates represented the necessary information or the steps of attack. The configuration file saved the detail information that attackers wanted, and the capabilities of attackers were stored in attacker profiles. In [11], Swiler *et al.* implements the method of [10] into a tool. Moreover, the elimination of redundant paths was also surmounted. Ammann *et al.* [12] developed a graph-based algorithm which was capable of finding mostly vulnerabilities. Ingols *et al.* [13] defined another attack graph which called MP attack graph. The graph where the nodes were classified three types. State nodes presented access levels of attackers on the hosts. Prerequisite nodes represented reachable hosts from state nodes. Vulnerability nodes presented vulnerabilities on the specific services.

More recently, Jha and Wing [18] proposed the attack graph to consider the network environment included the network user, IP address, running service, etc. In [8], [23]. Sheyner *et al.* defined the attack graph where each node denoted a state of the network systems and each edge denoted an atomic attack which changed state. They also added three configurations included system open port numbers, connection relations and vulnerabilities into the configuration file and used model checking tool called "NuSMV" [24] to analyze attack graph. Zhang *et al.* [14] expended the privilege into the attack graph and compared with [8]. The result proved that their graph was much simpler than that in [8]. The reason was that the model checking tool is not able to determine the privilege of the network system. From [15], Noel *et al.* defined another attack graph of network environment. Each node represented the machine on network and each edge represented the vulnerabilities that attackers used to compromise the network machine. Instead, the network machines were distributed to several subnets and then utilize the graph-drawing tool [25] to generate attack graph. This provided the good views for the administrators to know which subnets were easily

attacked. An architecture was proposed by Kotenko and Stepashkin [16] for security analysis based on construction of attack graph. In addition, they evaluated the network risk according to different wire network environment. Hence the attack graph not only to describe the vulnerabilities of the system but also to defend the environment of network before being attacked by attackers.

2.2 The Process of Risk Assessment

Risk assessment indicates the risks to network security and determines the probability of occurrence. Although it is impossible to use the risk assessment to eliminate all risks, administrators may expect the risks be reduced and adjust the configurations of the network environment.

According to [26], Gray *et al.* proposed the risk assessment process. The process was decomposed into nine parts and the flowchart is shown in Fig. 2.

- System characterization – In this step, the analysis items are identified, along with the configuration information and risk classifications that constitute the assessment model.
- Threat identification – The attacks of assessment environment are described in this step.
- Vulnerability identification – The goal of this step is to list the vulnerabilities that could be exploited by attackers.
- Control analysis – In this step, the rules is defined to describe the controllability or uncontrollability of the system after being attacked.
- Likelihood determination – The rules is defined to describe the probability of launching attacks.
- Impact analysis – In this step, the rules is defined to describe the impact severity of the system after being attacked.
- Risk determination – The goal of this step is to evaluate the security level of the system.

- Control recommendations – The goal of the recommended controls is to notice the security risks and support the experts to reduce the risks.
- Results documentations – Once the risk assessment has been completed, the results should be documented to help administrators understand the risks.

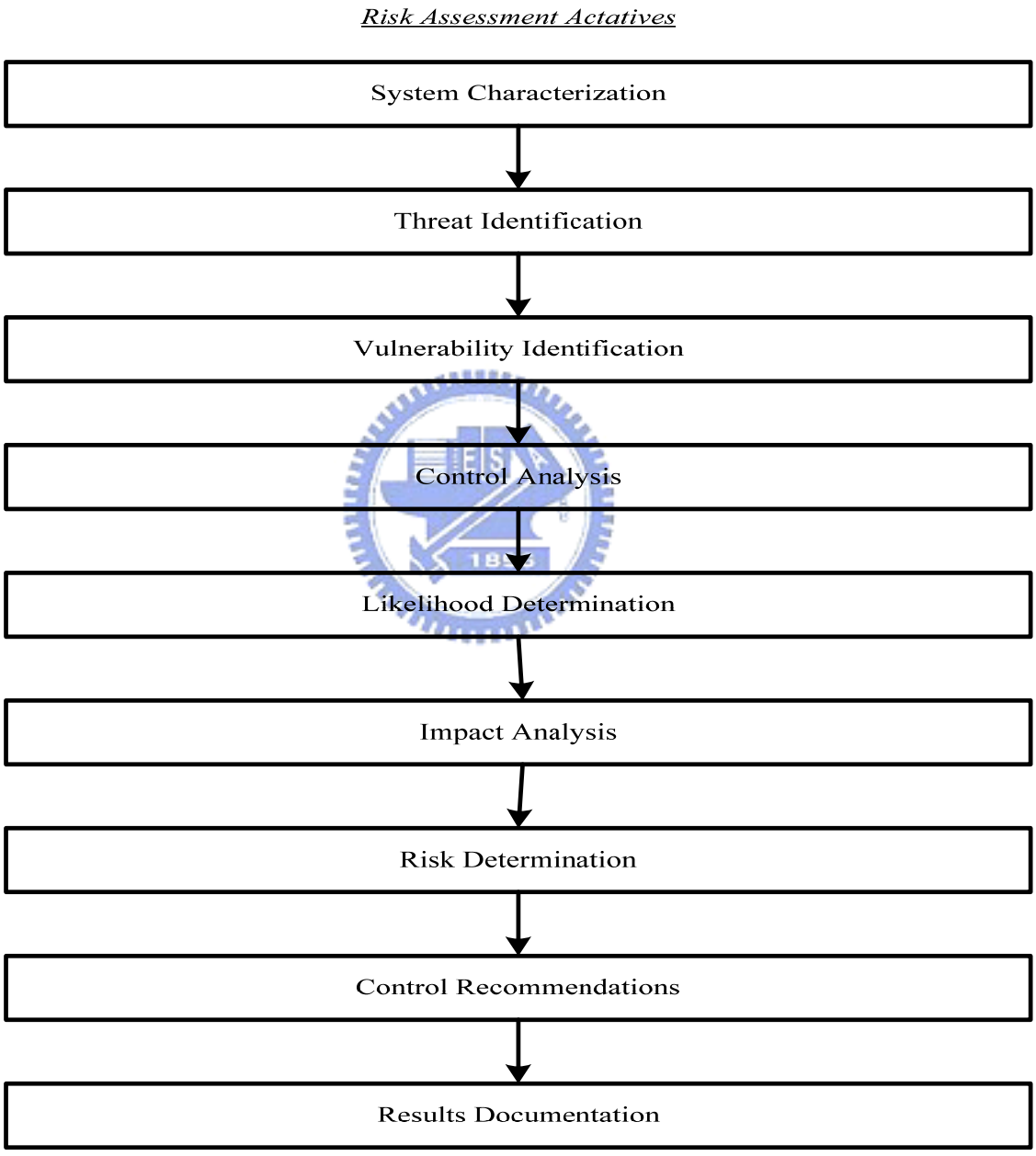


Fig. 2. Risk Assessment Methodology Flowchart (Gray *et al.* [26])

2.3 The Approaches of Risk Assessment

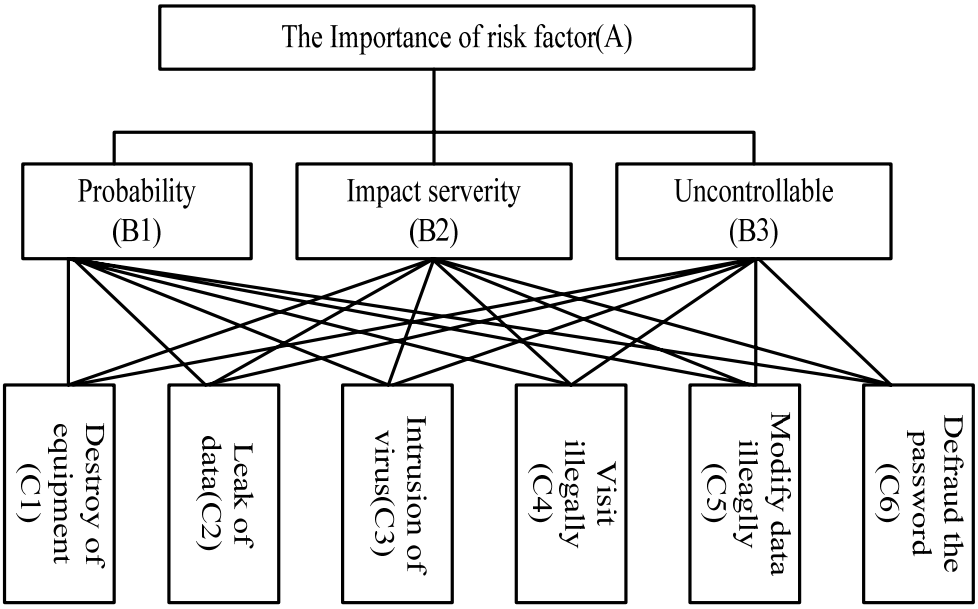


Fig. 3. The Hierarchy Structure of Risk Assessment (Zhao *et al.* [27], [28])

In [27], [28]. Zhao *et al*. designed a risk assessment architecture which depended on Gray's process as shown in Fig. 3. The top layer was the total risk value of network; the rules were defined in second layer and the network attacks were defined in the lowest layer. They also recommended a risk assessment method, which combined analytic hierarchy process (AHP) method and matrix operation for risk assessment. The steps of AHP method were specified as follow: (1) Constructing the hierarchy structure for risk assessment; (2) Constructing the judge matrix by expert experience; (3) Determining the weights of risk factors of each rule; (4) Calculating the quantitative coefficients depends on judge matrix. After finished the first three steps, they estimated the unknown probabilities of risk factors of each attack type, p_1, p_2, …, p_m, by using the Shannon entropy function [29] - [30]. This function was put forward to decide the weight of each network attack, as follows:

$$H = -\frac{1}{\ln^m}\sum_{i=1}^{m} p_i \ln p_i \qquad (1)$$

The judge matrix R of a rule is obtained by experts' experiences as well as a corresponding vector **b**, which represents weights of risk factors of the rule. Suppose that R is an n-by-m matrix in which n implies there are n attack types in the wireless environment, and m represents the number of the risk factors in the rule.

$$R = \begin{bmatrix} r_{11}\, r_{12} \cdots r_{1m} \\ r_{21}\, r_{22} \cdots r_{2m} \\ \vdots \quad \vdots \quad \quad \vdots \\ r_{n1}\, r_{n2} \cdots r_{nm} \end{bmatrix}$$

$$\mathbf{b} = [b_1, b_2, \ldots, b_m]^T$$

The weight vector, $\mathbf{q}^T$, **is** also acquired from the matrix by using Eq. (1).

$$\mathbf{q} = [q_1, q_2, \ldots, q_n]^T$$

Then the risk value of each rule can be calculated by the following equation:

$$r = \mathbf{q}^T \cdot R \cdot \mathbf{b} = \sum_{j=1}^{n} q_j \left(\sum_{k=1}^{m} r_{jk}\, b_k \right) \tag{2}$$

Changguang *et al.* [31] redesigned the architecture for wireless networks and used the same risk assessment method as [28]. They defined that the total risk value is the function of risk probability, impact severity and uncontrollability. The probability is denoted as p, the impact severity is denoted as c and uncontrollability is denoted as u, the risk happened denoted as s, whereas denoted as t. Then the formulas of total risk value can be calculated as:

$$\begin{aligned} R &= f(\textit{risk probability}, \textit{impact severity}, \textit{uncontrollable}) \\ &= 1 - p_t c_t u_t \\ &= 1 - (1 - p_s)(1 - c_s)(1 - u_s) \\ &= p_s + c_s + u_s - p_s c_s - p_s u_s - c_s u_s - p_s c_s u_s \end{aligned} \tag{3}$$

In [32], we know risk analysis could be analyzed through fuzzy linguistics; the information about risk was calculated via the fuzzy set theory and expressed in a natural language. However, the main drawback of the method is that it can not correctly calculate the average fuzzy set between two fuzzy sets. Therefore, Chen *et al.* [33] proposed an analysis method, which is called the center-of-gravity (COG) similarity method, to overcome the drawback of [32]. If the fuzzy value is not between zero and one, it is translated into the standardized fuzzy set. The average fuzzy set can be calculated by using fuzzy weight average (FWA) method shown as follows:

$$\tilde{R} = \frac{\sum_{i=1}^{n} \tilde{W}_i \times \tilde{R}_i}{\sum_{i=1}^{n} \tilde{W}_i} \tag{4}$$

Where $\tilde{R}$ is the average fuzzy set of the system security, $\tilde{W}_i$ and $\tilde{R}_i$ are the weight and the security risk level of each subsystem, respectively.

Liao *et al.* [34] proposed a hierarchical structure to construct the risk assessment architecture and used FWA method to compute the total risk value. The hierarchical structure was shown in Fig. 4, where each edge denoted fuzzy risk level and each node denoted weight importance of subsystem, respectively.

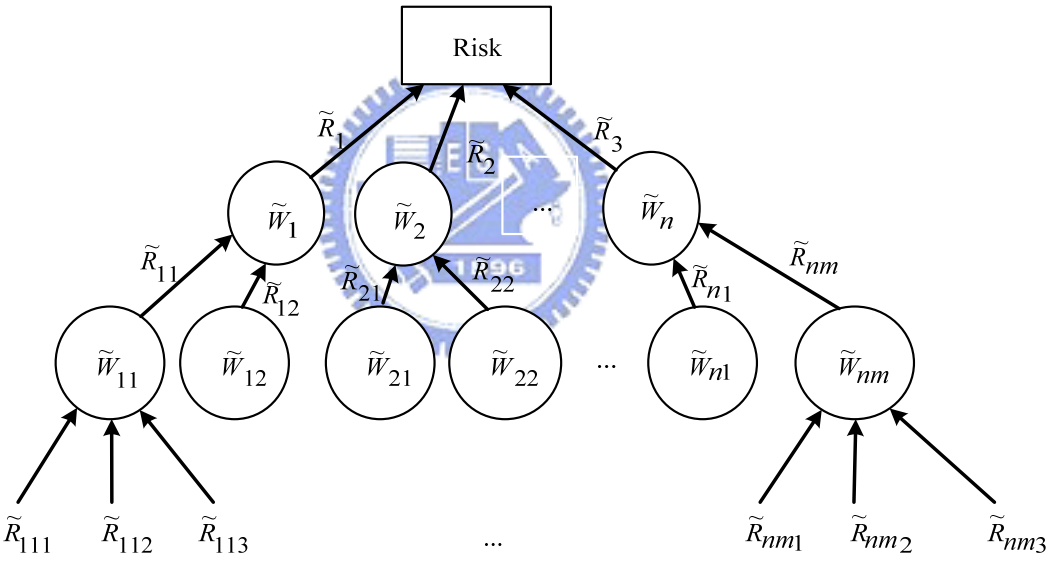


Fig. 4. Fuzzy Weight Average (FWA) Architecture (Liao *et al.* [27], [28])

The AHP method could easily obtain the quantitative value, but hardly constructed the judge matrixes if the analysis items changed with the environment. On the contrary, the linguistics method could easily extend the architecture, but hardly acquire the quantitative values.

Chapter 3

The Proposed Model for Risk Assessment

In this chapter, the proposed model is presented for risk assessment. In section 3.1, a hierarchical risk assessment architecture which combines the fuzzy linguistics and numerical descriptions is proposed to analyze the security robustness of wireless networks. Section 3.2 introduces the details of the attack types that we construct from the assessment architecture. In order to integrate fuzzy linguistics with numerical descriptions and calculate the risk value successfully, some definitions are described in section 3.3.

3.1 Constructing the Risk Assessment Architecture

According to the AHP method [26], [28], [32], the first step is to construct the risk assessment architecture of wireless networks. We can utilize layer structures to decompose complexity relationships into simple relationships. The highest layer is the goal, which is the total risk value of wireless environment. The second layer defines the same rule as [28]. The rule is judged in the aspects of probability of suffering attacked, impact severity and uncontrollability after being attacked. The third layer classifies the wireless attack types into six dimensions. Configurations in the lowest layer are the categories for wireless attack types that attackers will use when attacks occur. Fig. 5 shows the hierarchy risk assessment architecture of wireless networks.

As for the relationships among the architecture, we explain from the fourth layer to the top layer. The subcomponents of the fourth layer are represented by fuzzy linguistics which means the security weights of configurations and each edge is denoted the risk level between the configuration and the attack type. And then, the average fuzzy set of each attack type can be calculated through FWA method. By the expert experience, the risk degree between the

rules and the attack types can be decided. Hence we need to find the way to integrate fuzzy set and numerical value. In addition, according to [29], [30], the weights of attack types denote the discrepancies of experts. Hence we don't need to consider the influence of configurations, and we only need to use risk degrees to decide weights of attack types. By using Eq. (1), the weights of attack types can be calculated through these degrees.

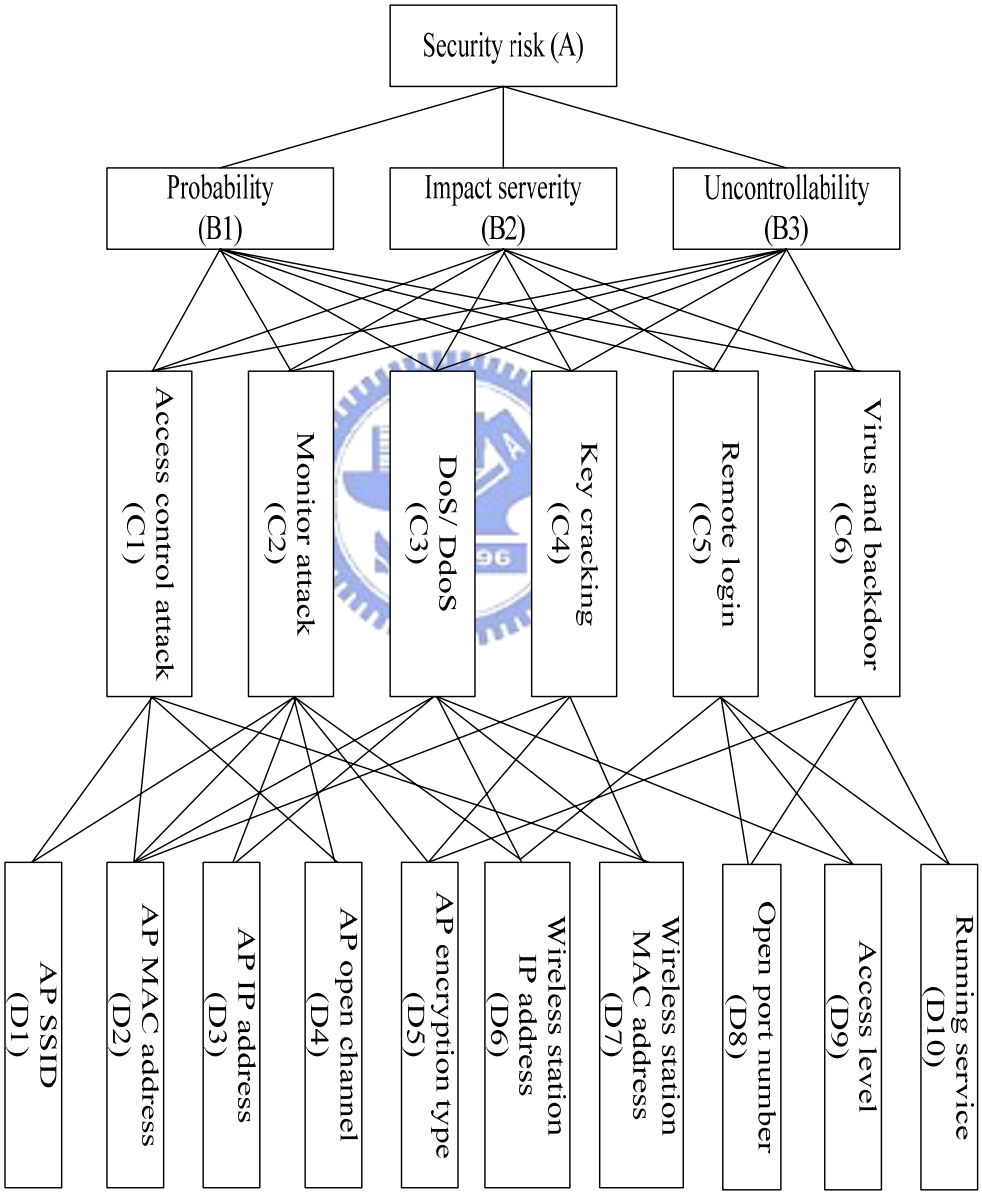


Fig. 5. The Assessment Architecture of the Wireless Networks

In order to combine fuzzy set with numerical value, the average fuzzy set should be quantified and then execute multiplication to the risk degree. The quantitative values of attack

types are called risk ratings. Attackers will get higher risk rating if they acquire more configurations. If we acquire quantitative risk ratings of n attack types, a_1, a_2, ..., a_n, the judge matrix can be modified where each row denotes the attack type and each column denotes the risk factor of the rule.

$$R' = \begin{bmatrix} a_1 r_{11} & a_1 r_{12} & \cdots & a_1 r_{1m} \\ a_2 r_{21} & a_2 r_{22} & \cdots & a_2 r_{2m} \\ \vdots & \vdots & & \\ a_n r_{n1} & a_n r_{n2} & \cdots & a_n r_{nm} \end{bmatrix}$$

Afterward the risk value of each rule can be modified as

$$r' = \sum_{j=1}^{n} q_j \left(\sum_{k=1}^{m} \alpha_j \, r_{jk} \, b_k \right) \tag{5}$$

Finally, according to Eq. (3), the total risk value can be calculated by matrix operations.

3.2 Classification of Attack Types

By the third layer of the risk assessment architecture, it classifies the attack types of wireless networks mainly include the following portions:

3.2.1 Access Control Attack

These attacks attempt to utilize the wireless resources which are not permitted by administrators. The description and the configurations of these attacks are shown in Table 1.

Table 1. Classification of Access Control Attack

Attack	Description	Configurations
Rouge access control	Installing an unsecured AP inside a network, and creating an open backdoor into trusted networks	AP SSID (D1) AP MAC address (D2) Open channel (D4)
MAC spoofing	Acquiring a legal MAC address to disguise as an authorized AP or station	STA MAC address (D7)

3.2.2 Monitor Attack

These attacks try to intercept aerial packets to obtain essential information concerned by attackers. The description and the configurations of these attacks are shown in Table 2.

Table 2. Classification of Monitor Attack

Attack	Description	Configurations
Eavesdropping	Capturing and decoding unprotected packets to obtain potentially sensitive information	AP IP address (D3), Encryption type (D5) STA IP address (D6)
Evil Twin AP	Masquerading as an authorized AP by beaconing the wireless service set identifier to lure users	AP SSID (D1) AP MAC address (D2) Open channel (D4)
Man in the Middle	Masquerading as an authorized AP and STA at one time, and collecting the packers between them	AP IP address (D3) Encryption type (D5) STA IP address (D6)

3.2.3 DoS/ DDoS Attack

These attacks are incidents which wireless stations and access points are interdicted of the services of the resource. The description and the configurations of these attacks are shown in Table 3.

Table 3. Classification of DoS/ DDoS attack

Attack	Description	Configurations
Authentication flood	Sending the forged authentication packets from random MAC addresses to fill a target AP's association table	AP MAC address (D2) STA MAC address (D7)
De-authentication flood	Flooding wireless stations by sending the forged de-authentication packets to disconnect users from an access point	AP MAC address (D2) STA MAC address (D7)
ICMP Ping Flood	Using attack tools to send a large ICMP packets to a wireless station or APs	AP IP address (D3) STA IP address (D6)

3.2.4 AP Key Cracking

These attacks try to decipher the encryption data to obtain the password which is configured by the access point. The description and the configurations of these attacks are shown in Table 4.

Table 4. Classification of AP Key Crack

Attack	Description	Configurations
WEP key cracking	Capturing packets to recover the WEP key by using WEP attack tools, such like aircrack, airsort.	AP MAC address (D2) Encryption type (D5) STA MAC address (D7)
WPA-PSK key cracking	Recovering the WPA key through captured key handshake frames by using dictionary attack tools, such like wpa_crack,, cWPAtty	AP MAC address (D2) Encryption type (D5) STA MAC address (D7)

Table 5. Classification of Remote Login

Attack	Description	Configurations
FTP	Filtering the FTP packets with the same source and destination addresses, comprising the packets to obtain the user id and password	STA IP address (D6) Open port number (D8) Access level (D9) Running service (D10)
Telnet	Filtering the Telnet session and examining the detail information to find the user id and password	STA IP address (D6) Open port number (D8) Access level (D9) Running service (D10)
Web	Consisting Web packets to acquire the essential browsing record and Web information	STA IP address (D6) Open port number (D8) Access level (D9) Running service (D10)

3.2.5 Remote Login

These attacks attempt to get the login id, the password, and other important information

in order to connecting with the remote hosts. The description and the configurations of these attacks are shown in Table 5.

3.2.6 Virus and Backdoors

These attacks attempt to infect some files to influence the hosts or let them open some services that attackers need. The description and the configurations of these attacks are shown in Table 6.

Table 6. Classification of Virus and Backdoor

Attack	Description	Configurations
Virus	Enticing the user to execute a virus program unwittingly and duplicated itself to infect another program in order to influence the hosts	Encryption type (D5) Open port number (D8) Running service (D10)
Backdoor	Attracting the user to execute a backdoor program unwittingly, controlling the compromised host that attackers need later	Encryption type (D5) Open port number (D8) Running service (D10)

3.3 Definition

In this section, we first define the composition of the fuzzy set and their arithmetic operations for the purpose of the risk assessment architecture. Also, a quantitative method of the fuzzy set, which extends the discrete fuzzy set, is proposed to determine the value of risk rating to integrate with expert experience.

Definition 1. Positive trapezoidal fuzzy set. *Suppose that a positive trapezoidal fuzzy set* $\tilde{A}(x)$ *can be represented as* (a_1,a_2,a_3,a_4)*, where* a_1,a_2,a_3 *and* a_4 *are real numbers, is described as any fuzzy subset with its membership function* $\mu_{\tilde{A}}(x)$ *is defined as follows and shown in*

Fig. 6.

$$\mu_{\tilde{A}}(x)=\begin{cases}\dfrac{x-a_1}{a_2-a_1} & a_1 \le x < a_2 \\ 1 & a_2 \le x < a_3 \\ \dfrac{a_4-x}{a_4-a_3} & a_3 \le x < a_4 \\ 0 & \text{others}\end{cases}$$

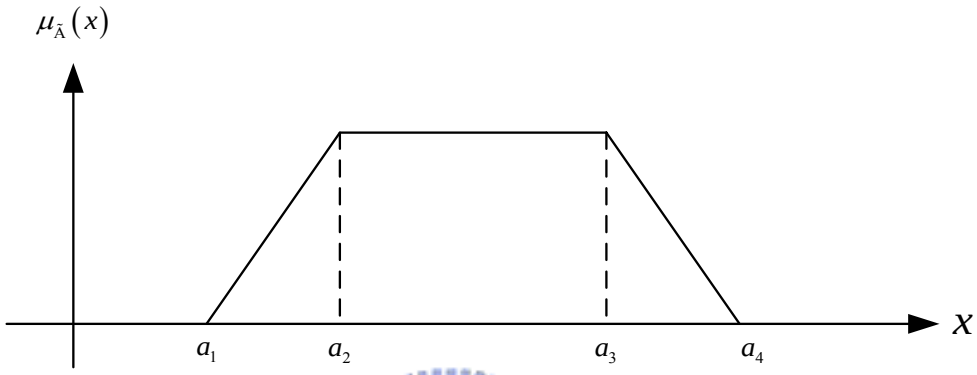


Fig. 6. Positive Trapezoidal Fuzzy Number

Where $\mu_{\tilde{A}}(x)$ indicates the membership value of the element x in $\tilde{A}$, and $\mu_{\tilde{A}}(x)\in[0,1]$.

From the Fig. 6, if $a_1 = a_2 = a_3 = a_4$, then $\tilde{A}(x)$ is called a real number. If $a_1 = a_2$ and $a_3 = a_4$, then $\tilde{A}(x)$ is called a crisp fuzzy set. If $a_2 = a_3$, then $\tilde{A}(x)$ is called a triangular fuzzy set.

Definition 2. Arithmetic operations of fuzzy sets. *For the two positive trapezoidal fuzzy sets* $\tilde{A}(x)$ *and* $\tilde{B}(x)$, *where* $\tilde{A}(x)=(a_1,a_2,a_3,a_4)$ *and* $\tilde{B}(x)=(b_1,b_2,b_3,b_4)$, *the arithmetic operations can be defined as follows.*

i) *Addition*:

$$\begin{aligned}\tilde{A}+\tilde{B}&=(a_1,a_2,a_3,a_4)+(b_1,b_2,b_3,b_4)\\&=(a_1+b_1,a_2+b_2,a_3+b_3,a_4+b_4)\end{aligned} \tag{6}$$

ii) *Subtraction*:

$$\begin{aligned}\tilde{A}-\tilde{B}&=(a_1,a_2,a_3,a_4)-(b_1,b_2,b_3,b_4)\\&=(a_1-b_4,a_2-b_3,a_3-b_2,a_4-b_1)\end{aligned} \tag{7}$$

iii) *Multiplication*:

$$\begin{aligned}\tilde{A}\times\tilde{B}=&\left[\ \min\left(a_1b_1,a_1b_4,a_4b_1,a_4b_4\right),\ \min\left(a_2b_2,a_2b_3,a_3b_2,a_3b_3\right),\right.\\&\left.\max\left(a_2b_2,a_2b_3,a_3b_2,a_3b_3\right),\max\left(a_1b_1,a_1b_4,a_4b_1,a_4b_4\right)\ \right]\\=&\left(a_1b_1,a_2b_2,a_3b_3,a_4b_4\right)\end{aligned}\tag{8}$$

iv) *Division*:

$$\begin{aligned}\tilde{A}/\tilde{B}=&\left[\ \min\left(a_1/b_1,a_1/b_4,a_4/b_1,a_4/b_4\right),\ \min\left(a_2/b_2,a_2/b_3,a_3/b_2,a_3/b_3\right),\right.\\&\left.\max\left(a_2/b_2,a_2/b_3,a_3/b_2,a_3/b_3\right),\max\left(a_1/b_1,a_1/b_4,a_4/b_1,a_4/b_4\right)\ \right]\\=&\left(a_1/b_4,a_2/b_3,a_3/b_2,a_4/b_1\right)\end{aligned}\tag{9}$$

Definition 3. Quantification of a fuzzy set. *For a bounded fuzzy set* $\tilde{A}(x)$, $f\left(\tilde{A}(x)\right)$ *is defined as the risk rating which means the distinction between a given fuzzy set and its fuzzy complement. For the set is defined within the interval* [0, 1]*, the quantification of the fuzzy set can be measured by:*

$$f\left(\tilde{A}(x)\right)=\int_0^1\left|2\tilde{A}(x)-1\right|dx\tag{10}$$

According to [35], Yager and Kirl introduced the fuzziness of the fuzz set $\tilde{A}(x)$ using the summation of the distinction which is measured by distance function between the fuzzy set and its fuzzy complement is defined as:

$$\begin{aligned}f\left(\tilde{A}(x)\right)=&\sum_{x\in X}\left(\left|\tilde{A}(x)-\tilde{A}^c(x)\right|\right)=\sum_{x\in X}\left(\left|\tilde{A}(x)-\left(1-\tilde{A}(x)\right)\right|\right)\\=&\sum_{x\in X}\left|2\tilde{A}(x)-1\right|\end{aligned}\tag{11}$$

Eq. (10) is suitable only to the discrete fuzzy set. However, the fuzzy set which is defined on the bounded fuzzy set can be readily modified. Consider the interval [0, 1]. The replacement results of Eq. (9) can be described in the following equation:

$$\begin{aligned}f\left(\tilde{A}(x)\right)=&\int_0^1\left|\tilde{A}(x)-\left(1-\tilde{A}(x)\right)\right|dx\\=&\int_0^1\left|2\tilde{A}(x)-1\right|dx\end{aligned}$$

□

Definition 4. Quantitative coefficient of the judge matrix. *For each judge matrix, the quantification coefficient* c_j, *which is the certainty of each attack type is defined as:*

$$c_j = 1 - e_j \tag{12}$$

where e_j is defined by Shannon's entropy measure [36] based on Eq. (1). The entropy e_j is the uncertainty of the given risk degrees and is defined as:

$$e_j = S(p_1, p_2, \ldots, p_m) = -\frac{1}{\ln m}\sum_{j=1}^{m} p_j \ln p_j \tag{13}$$

Definition 5. Normalized weight of the quantitative coefficient. *For the normalized weight* q_k, *each quantification coefficient* c_j *should be equally preferred. The formula is defined as:*

$$q_k = \frac{c_j}{\sum_{j=1}^{n} c_j} = \frac{1-e_j}{\sum_{j=1}^{n} 1-e_j} \tag{14}$$

Definition 6. Scope of the total risk value. For the total risk value R, $R \in [0,1]$, implies that the larger risk value reaches, the more danger of the wireless environment.

3.4 General Solution Algorithm

Our process of risk assessment is now almost complete, all that remains is to describe the calculating procedures with the steps in the analysis of wireless networks. In the following, we make some assumptions and then design a solution algorithm for risk assessment of wireless networks.

(1) We construct an m × n matrix to represent the configurations that the attack types utilize to start the attack. The rows denote the configurations and the columns denote the attack types. The matrix C is

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{bmatrix}$$

Remark. The matrix is boolean. If c_{ij} =1, it means that the j^{th} attack type needs the i^{th} configuration; whereas the j^{th} attack type doesn't need the i^{th} configuration.

(2) Suppose that the experts define a fuzzy linguistic representation vectors MF = [mf_1, mf_2, …, mf_k] of k elements, where each element includes four membership values.

(3) Suppose that the experts define a fuzzy risk levels vector L = [l_1, l_2,…, l_m] of m elements of the configurations, where each element includes four membership values.

(4) Suppose that there exists a vector R_v = [rv_1, rv_2,…, rv_k], where the i^{th} element denotes an n × q_i matrix. The rows represent the attack types and the columns represent the risk factors of each rule that defined by the experts.

(5) Suppose that there exists a vector B_v = [bv_1, bv_2,…, bv_k], where each element denotes a vector which means the weights of the risk factors that defined by experts. And the size of the i^{th} element is q_i.

The general solution algorithm is shown as follows:

Algorithm 3.1 Generalized Version for Risk Value Calculation

Input: A configuration file, config_file;
A m × n matrix C;
A risk level vector L of configurations of size m;
A vector R_V of size r, of which the ith element is an $n \times q_i$ matrix
A vector B_V of size r; of which the ith element is a vector of size q_i

Output: Risk value

Risk-Value-Calculate(*config_file*, C, L, R_V, B_V)
1 Read configurations from *config_file*

2 Let W be an array of size n

3 Set the weight value of each element of W according to the configurations and user's rules

4 Let R_C be an array of size n

5 **for** $i \leftarrow 1$ to n

6 **do** $mul \leftarrow 0$

7 $sum \leftarrow 0$

8 **for** $j \leftarrow 1$ to m

9 **do if** $C[j, i] = 1$ ► Check if the j^{th} configuration is used by the i^{th} attack type

10 **then** $mul \leftarrow mul + W[j] \cdot L[j]$

11 $sum \leftarrow sum + W[j]$

12 $R_C[i] \leftarrow mul / sum$

13 let F be an array of size n

14 **for** $i \leftarrow 1$ to n

15 **do** $F[i] \leftarrow$ integrate $|(2R_C[i])-1|$ from 0 to 1

16 let c_V be a vector of size r, of which the element is a vector of size n

17 let q_V be a vector of size r, of which the element is a vector of size n

18 **for** $i \leftarrow 1$ to r

19 **do** $R \leftarrow R_V[i]$

20 $c \leftarrow c_V[i]$

21 $q \leftarrow q_V[i]$

22 $sum \leftarrow 0$

23 **for** $j \leftarrow 1$ to n

24 **do** $e \leftarrow 0$

25 **for** $k \leftarrow 1$ to columns[R]

26 **do** $R[j, k] \leftarrow F[j] \cdot R[j, k]$

27 $e \leftarrow e + (R[j, k]/ F[j]) \cdot \ln (R[j, k]/ F[j])$

28 e $\leftarrow -e / \ln$ columns[R]

29 $c[j] \leftarrow 1 - e$

30 $sum \leftarrow sum + c[j]$

31 **for** $j \leftarrow 1$ to n

32 **do** $q[j] \leftarrow c[j] / sum$

33 Let Rr be a vector of size r

34 **for** $i \leftarrow 1$ to r

35 **do** Rr$[i] \leftarrow q_V[i]^T R_V[i] \; b_V[i]$

36 use the risk value of each rule, $Rr[i]$, to calculate the total risk value, *risk*

37 **return** *risk*

Suppose that experts define three rules, probability before being attacked (p_s), impact severity after being attacked (i_s) and system uncontrollability after being attacked (u_s), to determine the total risk of a system. There are w risk factors of probability, x risk factors of impact severity, and y risk factors of uncontrollability. If there are n attack types of assessment architecture, then the proposed approach has the following property.

Property: if an attacker obtains more information of the environment E1 than that of the environment E2, then the risk existing in E1 is larger than that in E2.

Proof.

If an attacker obtains more configurations of the wireless environment E1 than that of E2, according to experts' experience, E1's rating vector, α, is indeed larger than E2's rating vector, α', where

$$\alpha = [\alpha_1, \alpha_2, \cdots, \alpha_n]^T, \alpha' = [\alpha'_1, \alpha'_2, \cdots, \alpha'_n]^T.$$

Assume that without loss of generality that $\alpha_i > \alpha_i'$ and all the other rating elements in α and α', are the same, i.e. $\alpha_j = \alpha_j'$ $\forall j = 1, 2, 3, \ldots, n$ and $j \neq i$.

By the definitions and algorithm steps introduced in Chapter 3, three judge matrixes, R_p, R_i, and R_u, are obtained by experts' experiences as well as the corresponding vectors, $\mathbf{b_p}$, $\mathbf{b_i}$ and $\mathbf{b_u}$, which represent weights of risk factors of the three rules.

$$R_p = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1w} \\ r_{21} & r_{22} & \cdots & r_{2w} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nw} \end{bmatrix} \qquad R_i = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1x} \\ r_{21} & r_{22} & \cdots & r_{2x} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nx} \end{bmatrix} \qquad R_u = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1y} \\ r_{21} & r_{22} & \cdots & r_{2y} \\ \vdots & \vdots & & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{ny} \end{bmatrix}$$

$\mathbf{b_p} = [b_{p1}, b_{p2}, \ldots, b_{pw}]^T$, $\mathbf{b_i} = [b_{i1}, b_{i2}, \ldots, b_{ix}]^T$, and $\mathbf{b_u} = [b_{u1}, b_{u2}, \ldots, b_{uy}]^T$.

Three weight vectors, $\mathbf{c_p}^T$, $\mathbf{c_i}^T$, and $\mathbf{c_u}^T$, are also acquired from the matrixes,

where $\mathbf{c_p} = [c_{p1}, c_{p2}, \ldots, c_{pn}]^T$, $\mathbf{c_i} = [c_{i1}, c_{i2}, \ldots, c_{in}]^T$, and $\mathbf{c_u} = [c_{u1}, c_{u2}, \ldots, c_{un}]^T$,

$$c_{pj} = 1 - \left(\frac{-1}{\ln^q} \sum_{k=1}^{w} r_{jk} \ln r_{jk} \right), \qquad 0 \le c_{pj} \le 1$$

$$c_{ij} = 1 - \left(\frac{-1}{\ln^s} \sum_{k=1}^{x} r_{jk} \ln r_{jk} \right), \qquad 0 \le c_{ij} \le 1$$

$$c_{uj} = 1 - \left(\frac{-1}{\ln^t} \sum_{k=1}^{y} r_{jk} \ln r_{jk} \right), \qquad 0 \le c_{uj} \le 1$$

Then we can obtain three normalized weight vectors, $\mathbf{q_p}^T$, $\mathbf{q_i}^T$, and $\mathbf{q_u}^T$, where $\mathbf{q_p} = [q_{p1}, q_{p2}, \ldots, q_{pn}]^T$, $\mathbf{q_i} = [q_{i1}, q_{i2}, \ldots, q_{in}]^T$, and $\mathbf{q_u} = [q_{u1}, q_{u2}, \ldots, q_{un}]^T$,

$$q_{pj} = \frac{c_{pj}}{\sum_{j=1}^{n} c_{pj}}, \qquad 0 \le q_{pj} \le 1$$

$$q_{ij} = \frac{c_{ij}}{\sum_{j=1}^{n} c_{ij}}, \qquad 0 \le q_{ij} \le 1$$

$$q_{uj} = \frac{c_{uj}}{\sum_{j=1}^{n} c_{uj}}, \qquad 0 \le q_{uj} \le 1$$

Given the above vectors and matrixes, in the environment E1, p_s (the probability of suffering attacked), i_s (the impact severity after being attacked) and c_s (the uncontrollability after being attacked) are determined.

$$p_s = \sum_{j=1}^{n} q_{pj} \left(\sum_{k=1}^{w} \alpha_j r_{jk} b_{pk} \right), \qquad 0 \le p_s \le 1$$

$$i_s = \sum_{j=1}^{n} q_{ij} \left(\sum_{k=1}^{x} \alpha_j r_{jk} b_{ik} \right), \qquad 0 \le i_s \le 1$$

$$u_s = \sum_{j=1}^{n} q_{uj} \left(\sum_{k=1}^{y} \alpha_j r_{jk} b_{uk} \right), \qquad 0 \le u_s \le 1$$

Similarly, the three corresponding values of the environment E2 are determined.

$$p'_s = \sum_{j=1}^{n} q_{pj} \left(\sum_{k=1}^{w} \alpha'_j r_{jk} b_{pk} \right), \qquad 0 \le p'_s \le 1$$

$$i'_s = \sum_{j=1}^{n} q_{ij} \left(\sum_{k=1}^{x} \alpha'_j r_{jk} b_{ik} \right), \qquad 0 \le i'_s \le 1$$

$$u'_s = \sum_{j=1}^{n} q_{uj} \left(\sum_{k=1}^{y} \alpha'_j r_{jk} b_{uk} \right), \qquad 0 \le u'_s \le 1$$

Finally, by Eq. (3), we can get R and R', the total risks existing in the environment E1 and E2, respectively.

R=1-(1-p_s)* (1-i_s)* (1-u_s), and R'=1-(1-p_s')*(1-i_s')* (1-u_s').

$\because$ $\alpha_i > \alpha'_i$ and all the other rating elements in α and α' are the same,

$\therefore p_s > p'_s$, $i_s > i'_s$ and $u_s > u'_s$ and thus derives that R>R'.

Hence, it is proved that the more configurations attackers acquire the more risk exists in the wireless environment.

Chapter 4

Examples

In this chapter, two graph-based risk assessment examples with different configurations of wireless networks are given as a demonstration of the application of the proposed method in realistic scenarios. The total risk value between an access point and a wireless station is calculated in section 4.1. Section 4.2 extends the first example and introduces how to calculate the total risk value between two wireless stations.

4.1 Calculating Risk Value between AP and Station

In this section, we first introduce the wireless environment between an assess point and a wireless station in this example. In order to accomplish our purpose, the AHP rule depiction and the fuzzy linguistic rule depiction will be presented in order to compute the total risk value. Finally, the result will be calculated according to these assessment rules and shown in attack graph.

4.1.1 The Environment of Wireless Network

According to [9]-[23], each device should contain relevant information in configurations to help administrators analyze the security robustness of wireless networks. Hence consider a wireless network example shown in Fig. 7. There are two wireless devices, an access point (AP1) and a wireless station (STA1), STA1 has already connected with AP1. Suppose that the configurations of these two devices have been detected, and we want to calculate the total risk value between them. As shown, the configurations of the two devices can be utilized to analyze the risk of the wireless network.

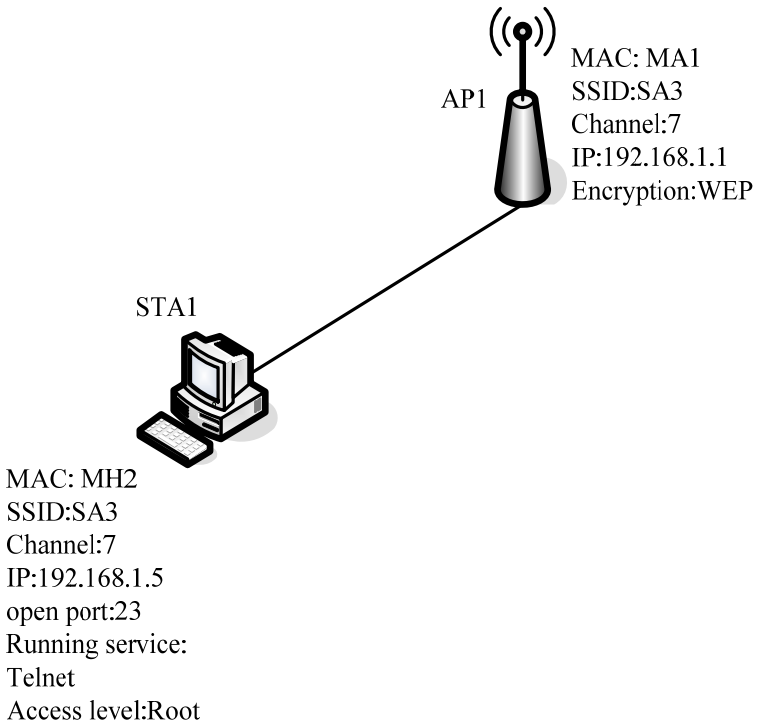


Fig. 7.Wireless Network Example (AP and station)

4.1.2 Determination of the Analysis Rules

From the security risk analysis [22], the analysis rule must be constructed for risk value computation. Therefore, the AHP rules and fuzzy linguistic rule should be constructed for our risk computation according to Fig. 5. The procedures of rules construction are decomposed as follows:

Step 1. Determine the Risk Factors of Each Rule — From Fig. 5, the rules of the second layer are constructed as probability, impact severity, and uncontrollability. According to the AHP method [27]-[28], it is necessary to design the risk factors, and risk weight of each rule. Because Zhao *et al.*[27] have designed the risk factors by the experts, thus we use the same risk factors as theirs. Suppose the risk factor set is $V = \{V_1, V_2, \ldots, V_m\}$, then the rule factors of each rule is shown in Table 7.

Table 7. The Risk Factors of Each Rule

Rule / Factor	Probability	Impact severity	Uncontrollability
V_1	Negligible	Insignificant	Controllable
V_2	Very low	Monitor	Controllable mainly
V_3	Low	Significant	Uncontrollable
V_4	Medium	Serious	Undefined
V_5	High	Critical	Undefined
V_6	Very high	Undefined	Undefined
V_7	Extreme	Undefined	Undefined

Step 2. Determine the Risk Degrees and Risk Weight — According to above discussion, we should determine the risk weight of each risk factor of each rule. Of course, the weights satisfy uniform condition. Furthermore, the risk degree between each risk factor in the layer 2 and each attack type in the layer 3 should also be decided. Suppose the experts make assessment tables of the probability (B_1), impact severity (B_2), and uncontrollability (B_3). The tables which include the risk weights and the risk degrees are shown in Table 8, Table 9, and Table 10.

Table 8. Risk Degree and Risk Weight of Probability

Layer 3 / Layer 2		Attack type						Weight of risk factor
		C_1	C_2	C_3	C_4	C_5	C_6	
Risk factor	V_1	0.00	0.00	0.00	0.00	0.00	0.10	1/49
	V_2	0.00	0.00	0.00	0.00	0.00	0.10	3/49
	V_3	0.00	0.00	0.00	0.00	0.00	0.10	5/49
	V_4	0.40	0.10	0.00	0.00	0.00	0.20	7/49
	V_5	0.30	0.20	0.50	0.10	0.10	0.30	9/49
	V_6	0.20	0.40	0.40	0.50	0.40	0.20	11/49
	V_7	0.10	0.30	0.10	0.40	0.50	0.00	13/49

Table 9. Risk Degree and Risk Weight of Impact Severity

Layer 3 / Layer 2		Attack type						Weight of risk factor
		C_1	C_2	C_3	C_4	C_5	C_6	
Risk factor	V_1	0.00	0.10	0.10	0.00	0.00	0.00	1/25
	V_2	0.30	0.10	0.00	0.00	0.00	0.10	3/25
	V_3	0.40	0.10	0.40	0.10	0.00	0.20	5/25
	V_4	0.30	0.30	0.30	0.20	0.40	0.50	7/25
	V_5	0.00	0.40	0.20	0.70	0.60	0.20	9/25

Table 10. Risk Degree and Risk Weight of Uncontrollability

Layer 3 / Layer 2		Attack type						Weight of risk factor
		C_1	C_2	C_3	C_4	C_5	C_6	
Risk factor	V_1	0.00	0.30	0.60	0.10	0.10	0.50	1/9
	V_2	0.40	0.50	0.40	0.30	0.40	0.50	3/9
	V_3	0.60	0.20	0.00	0.60	0.50	0.00	5/9

Step 3. Fuzzy Linguistic Terms Representation — Since the configurations of wireless environment are represented by fuzzy linguistics, we apply night-member linguistic terms which are expressed in positive trapezoidal sets to deal with the weights and the risk levels of configurations, as shown in Table 11.

Table 11. A Nine-Member Linguistic Term Set

Linguistic Term	Trapezoidal Fuzzy Numbers
Absolute low (AL)	(0.00, 0.00, 0.00, 0.00)
Very low (VL)	(0.00, 0.00, 0.02, 0.07)
Low (L)	(0.04, 0.10, 0.18, 0.23)
Fairly low (FL)	(0.17, 0.22, 0.36, 0.42)
Medium (M)	(0.32, 0.41, 0.58, 0.65)
Fairly high (FH)	(0.58, 0.63, 0.80, 0.86)
High (H)	(0.72, 0.78, 0.92, 0.97)
Very high (VH)	(0.93, 0.98, 1.00, 1.00)
Absolute high (AH)	(1.00, 1.00, 1.00, 1.00)

Step 4. Design Rules for Weights of the Configurations — After deciding the linguistic terms representation, then the fuzzy analysis rules can be designed according to Table 11. We design three rules for weights of configurations. The first fuzzy linguistic rule, shown in Table 12, is to express the capability on access levels of attackers. Table 13 shows the second rule that it uses linguistic terms to express the running service whether it has encrypted for data transmission or not.

Table 12. Linguistic Term for Access Level of Attacker

Access level of attackers	Linguistic term
Root	AH
User	FH
Guest	FL
None	AL

Table 13. Linguistic Term for Data Encryption of Running Service

Data encryption of running service	Linguistic term
None encryption (plain text)	VH
Encryption (cipher text)	M
Undetected	VL

As for the third rule, we focus on safety and acquirable probability of the other configurations that can be obtained from wireless packets. According to IEEE standards [37], we can classify configurations themselves through the safety of wireless encrypted types; and the acquirable probabilities of configurations are classified through encrypted types of access points. We group the safety and the acquirable probability into four levels, as shown in Table 14 and Table 15, respectively. By applying Table 14 and Table 15, the third fuzzy linguistic rule can be subjectively designed and shown in Table 16. If attackers can not get the

information of configuration, the weight was set absolute low (AL). It means the risk is absolute low; otherwise, the weight of configuration is decided according to the three rules.

Table 14. Safety of Encrypted Type

Encrypted type of configurations	Safety
None encryption	None
WEP	Low
WPA-PSK	Medium
Others	High

Table 15. Probability of Gather Configurations

Encrypted type of access point	Acquirable probabilities of configurations
None encryption	High: D_1, D_2, D_3, D_5, D_6, D_7, D_8
	Medium: D_4
	Low:
	Impossible:
WEP encryption	High: D_1, D_2, D_7
	Medium: D_3, D_4, D_5, D_6, D_8
	Low:
	Impossible:
WPA-PSK encryption	High: D_1, D_2, D_7
	Medium: D_4
	Low: D_3, D_5, D_6, D_8
	Impossible:
Others	High: D_1, D_2, D_7
	Medium: D_4
	Low:
	Impossible: D_3, D_5, D_6, D_8

Step 5. Design Rule for Risk Levels of the Configurations — As former discussion from Table 1 to Table 6, suppose that the risk levels of configurations are resolved according to the

number of times that each configuration is applied on wireless attacks by attackers, as shown in Table 17.

Table 16. Linguistic Term for Safety and Acquirable Probability of Configuration

Encrypted type of configurations	Acquirable probability of configurations			
	High	Medium	Low	Impossible
None (None encryption)	VH	H	FH	M
Low (WEP)	H	FH	M	FL
Medium (WPA-PSK)	FH	M	FL	L
High (Others)	M	FL	L	VL

Table 17. Linguistic Term for Risk Level of Configuration

Applied time of configuration	Linguistic term
7	VH
6	H
5	FH
4	M
3	FL
2	L
1	VL

4.1.3 Algorithm

After determining the analysis rules, the algorithm in this example can be designed to explain how to calculate the risk value between an access point and a station. We should take three assumptions in order to finish the algorithm.

(1) Suppose that there exists three-analysis rule of probability, impact severity, and uncontrollability. There are q risk factors of the probability, r risk factors of impact severity, and s risk factors of uncontrollability. The experts give risk degree between each rule and each attack type, then the matrixes R_p, R_i, and R_u can be constructed where the rows denote

the attack types and the columns denote the risk factors. They are

$$R_p = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1q} \\ r_{21} & r_{22} & \cdots & r_{2q} \\ \vdots & \vdots & \cdots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nq} \end{bmatrix} \qquad R_i = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1s} \\ r_{21} & r_{22} & \cdots & r_{2s} \\ \vdots & \vdots & \cdots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{ns} \end{bmatrix} \qquad R_u = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1t} \\ r_{21} & r_{22} & \cdots & r_{2t} \\ \vdots & \vdots & \cdots & \vdots \\ r_{n1} & r_{n2} & \cdots & r_{nt} \end{bmatrix}$$

(2) Suppose that there exists three vectors $b_p = [b_1, b_2, \ldots, b_q]$, $b_i = [b_1, b_2, \ldots, b_s]$, and $b_u = [b_1, b2, \ldots, b_t]$.The vectors represent the weights of the risk factors.

(3) Suppose that there exists a vector $W = [w_1, w_2, \ldots, w_k]$ of k elements, where each element includes four membership values to describe the weight of each configuration.

From Fig. 5, there are 6 attack types and 3 rules where q is equal to 7, r is equal to 5 and s is equal to 3 according to Table 7. In this example, there are 10 configurations consisted of AP1and STA1. The fuzzy linguistic representation vectors MF = [AL, VL, L, FL, M, FH, H, VH, AH] is constructed according to Table 11, and then we can modify the algorithm 3.1 and generate two algorithms. The first algorithm describes how to obtain the total risk value; the other one represents weights of the configurations as follows.

Algorithm 4.1 Risk Value Calculation

Input: A configuration file, config_file;
A 15 × 6 matrix C;
A risk level vector L of configurations of size 15;
A 6 × 7 matrix R_p;
A 6 × 5 matrix R_i;
A 6 × 3 matrix R_u;
A vector b_p of size 7;
A vector b_i of size 5;
A vector b_u of size 3

Output: Risk value

Risk-Value-Calculate (*config_file*, C, L, R_p, R_i, R_u, b_p, b_i, b_u)

1 $W \leftarrow$ GET-WEIGHTS (*config_file*)
2 Let R_C be an array of size 6
3 **for** $i \leftarrow 1$ to 6
4 **do** $mul \leftarrow 0$

```
5                   sum ← 0
6                   for j ← 1 to length[W]
7                       do if C[j, i] = 1
8                           then mul ←mul + W[j] · L[j]
9                                sum ← sum + W[j]
10                  R_C[i] ← mul / sum
11          Let F be an array of size 6
12          for i ← 1 to 6
13              do F[i] ← integrate |(2R_C[i])-1| from 0 to 1
14              ► Modify judge matrix R_p and obtain quantitative coefficient vector q_p
15          Let c_p be a vector of size 6
16          sum_p ← 0
17          for i ← 1 to 6
18              do e_p ← 0
19                  for j ← 1 to 7
20                      do R_p[i, j] ← F[i] · R_p[i, j]
21                          e_p ← e_p + (R_p[i, j]/ F[i]) · ln (R_p[i, j]/ F[i])
22                  e_p ← (-e_p / ln 7)
23                  c_p[i] ← 1 - e_p
24                  sum_p ← sum_p + c_p[i]
25              ► Modify judge matrix R_i and obtain quantitative coefficient vector q_i
26          Let c_i be a vector of size 6
27          sum_i ← 0
28          for i ← 1 to 6
29              do e_i ← 0
30                  for j ← 1 to 5
31                      do R_i [i, j] ← F[i] · R_i [i, j]
32                          e_i ← e_i + (R_p[i, j]/ F[i]) · ln (R_p[i, j]/ F[i])
33                  e_i ← (-e_i / ln 5)
34                  c_i [i] ← 1 - e_i
35                  sum_i ← sum_i + c_i [i]
36              ► Modify judge matrix R_u and obtain quantitative coefficient vector c_u
37          Let c_u be a vector of size 6
38          sum_u ← 0
39          for i ← 1 to 6
40              do e_u ← 0
41                  for j ← 1 to 3
42                      do R_u [i, j] ← F[i] · R_u [i, j]
```

$e_u \leftarrow e_u + (R_p[i, j]/ F[i]) \cdot \ln (R_p[i, j]/ F[i])$

$e_u \leftarrow (-e_u / \ln 3)$

$c_u [i] \leftarrow 1 - e_u$

$sum_u \leftarrow sum_u + c_u [i]$

► Calculate quantitative weight vectors q_p, q_i, and q_u

Let q_p, q_i, q_u be a vector of size 6

for $i \leftarrow 1$ to 6

do $q_p[i] \leftarrow c_p[i] / sum_p$

$q_i[i] \leftarrow c_i[i] / sum_i$

$q_u[i] \leftarrow c_u[i] / sum_u$

$p_s \leftarrow q_p^T R_p b_p$

$c_s \leftarrow q_i^T R_i b_i$

$u_s \leftarrow q_u^T R_u b_u$

$risk \leftarrow p_s + c_s + u_s - p_s \cdot c_s - p_s \cdot u_s - c_s \cdot u_s - p_s \cdot c_s \cdot u_s$

return *risk*

Algorithm 4.2 Getting Weights

Input: A configuration file, *config_file*;

Output: An array *W* which stores the weight value of each configuration

GET-WEIGHTS(*config_file*)

read the type of this configuration file from *config_file*, and then set *config_file_type*

read configurations from *config_file*, including *ap_ssid*, *ap_mac_addr*, *ap_ip_addr*, *ap_channel*, *ap_encryption*, *sta1_mac_addr*, *sta1_ip_addr*, *sta1_port*, *sta1_access_level* and *sta1_running_service*

if *config_file_type* = STAs

then read extra configurations from *config_file*, including *sta2_mac_addr*, *sta2_ip_addr*, *sta2_port*, *sta2_access_level* and *sta2_running_service*

allocate an array *W* of size 15 dynamically

else allocate an array *W* of size 10 dynamically

► Get weight between access level and attack types

if *sta1_access_level* = root

then *W*[9] ← *MF*[9]

elsif *sta1_access_level* = user

then *W*[9] ← *MF*[6]

elsif *sta1_access_level* = guest

then *W*[9] ← *MF*[4]

else *W*[9] ← *MF*[1]

11 **if** *config_file_type* = STAs
12 **then if** *sta2_access_level* = root
13 **then** *W*[14] ← *MF*[9]
14 **elsif** *sta2_access_level* = user
15 **then** *W*[14] ← *MF*[6]
16 **elsif** *sta2_access_level* = guest
17 **then** *W*[14] ← *MF*[4]
18 **else** *W*[14] ← *MF*[1]
19 ► Get weight between running service and attack types
19 **if** *sta1_running_service* is un-encryption
20 **then** *W*[10] ← *MF*[8]
21 **elsif** *sta1_running_service* is encryption
22 **then** *W*[10] ← *MF*[5]
23 **else** *W*[10] ← *MF*[2]
11 **if** *config_file_type* = STAs
24 **then if** *sta2_running_service* is un-encryption
25 **then** *W*[15] ← *MF*[8]
26 **elsif** *sta2_running_service* is encryption
27 **then** *W*[15] ← *MF*[5]
28 **else** *W*[15] ← *MF*[2]
29 ► Get weights between other configurations and attack types
30 **if** *ap_encryption* = NIL
31 **then** *W*[1] ← *W*[2] ← *W*[3] ←*W*[5] ← *W*[6] ← *W*[7] ← *W*[8] ←*MF*[8]
32 *W*[4] ← *MF*[7]
if *config_file_type* = STAs
then *W*[11] ← *W*[12] ← *W*[13] ← *MF*[8]
34 **elsif** *ap_encryption* = WEP
35 **then** *W*[1] ← *W*[2] ← *W*[7] ← *MF*[8]
36 *W*[3] ← *W*[4] ← *W*[5] ← *W*[6] ← *W*[8] ← *MF*[7]
if *config_file_type* = STAs
then *W*[12] ← *MF*[8]
W[11] ← *W*[13] ← *MF*[7]
37 **elsif** *ap_encryption* = WPA-PSK
38 **then** *W*[1] ← *W*[2] ← *W*[7] ← *MF*[8]
39 *W*[4] ← *MF*[7]
40 *W*[3] ←*W*[5] ← *W*[6] ← *W*[8] ← *MF*[4]
if *config_file_type* = STAs
then *W*[12] ← *MF*[7]
W[11] ← *W*[13]← *MF*[4]

```
41      else W[1] ← W[2] ← W[7] ← MF[8]
42           W[4] ← MF[7]
43           W[3] ←W[5] ← W[6] ← W[8] ← MF[2]
             if config_file_type = STAs
                  then W[12] ← MF[7
                       W[11] ← W[13]← MF[2]
44           ► Set weight of configuration to MF[1] if the configuration is not available
45      if ap_ssid = NIL
46           then W[1] ← MF[1]
47      if ap_mac_addr = NIL
48           then W[2] ← MF[1]
49      if ap_ip_addr = NIL
50           then W[3] ← MF[1]
51      if ap_channel = NIL
52           then W[4] ← MF[1]
53      if ap_encryption = NIL
54           then W[5] ← MF[1]
55      if sta1_ip_addr = NIL
56           then W[6] ← MF[1]
57      if sta1_mac_addr = NIL
58           then W[7] ← MF[1]
59      if sta1_port = NIL
60           then W[8] ← MF[1]
11      if config_file_type = STAs
61           then if sta2_ip_addr = NIL
62                     then W[11] ← MF[1]
63                if sta2_mac_addr = NIL
64                     then W[12] ← MF[1]
65                if sta2_port = NIL
66                     then W[13] ← MF[1]
67      return W
```

4.1.4 Evaluation

In the following, we use the proposed risk assessment method to explain the risk assessment processes of the wireless network. The procedures are decomposed into six steps as follows:

(1) **Constructing the security list table —** According to the configurations of Fig. 1, we can construct linguistic security lists which include the weights and risk levels of the configurations base on Table 12, Table 13, Table 16 and Table 17, as shown in Table 18.

Table 18. Linguistic List of the Weight and the Risk Level (AP1 and STA1)

Configuration		Attack type						Risk level
		C_1	C_2	C_3	C_4	C_5	C_6	
AP1	D_1	VH	VH					L
	D_2	VH	VH	VH	VH			H
	D_3		FH	FH				FL
	D_4	H	H					L
	D_5		FH		FH		FH	H
STA1	D_6		FH	FH				H
	D_7	VH		VH	VH	VH		FH
	D_8					FH	FH	FH
	D_9			AH		AH		FL
	D_{10}					VH	VH	FH

(2) **Calculating the fuzzy average set —** By using FWA method and fuzzy arithmetic operation from Eq. (4) and Eqs. (6) to (9), we can obtain the average fuzzy set of each attack type:

$$\begin{aligned}
\tilde{R}_{C_1} &= \left[\tilde{W}_{D1}\times\tilde{R}_{D1}+\tilde{W}_{D2}\times\tilde{R}_{D2}+\tilde{W}_{D4}\times\tilde{R}_{D4}+\tilde{W}_{D7}\times\tilde{R}_{D7}\right]/\left[\tilde{W}_{D1}+\tilde{W}_{D2}+\tilde{W}_{D4}+\tilde{W}_{D7}\right] \\
&= \left[\mathrm{VH}\times\mathrm{L}+\mathrm{VH}\times\mathrm{H}+\mathrm{H}\times\mathrm{L}+\mathrm{VH}\times\mathrm{FH}\right]/\left[\mathrm{VH}+\mathrm{VH}+\mathrm{H}+\mathrm{H}\right] \\
&= \big[\ (0.93, 0.98, 1.00, 1.00)\times(0.04, 0.10, 0.18, 0.23) \\
&\quad +(0.93, 0.98, 1.00, 1.00)\times(0.72, 0.78, 0.92, 0.97) \\
&\quad +(0.72, 0.78, 0.92, 0.97)\times(0.04, 0.10, 0.18, 0.22) \\
&\quad +(0.93, 0.98, 1.00, 1.00)\times(0.58, 0.63, 0.80, 0.86)\big] \\
&\quad /\big[(0.93, 0.98, 1.00, 1.00)+(0.93, 0.98, 1.00, 1.00) \\
&\quad +(0.72, 0.78, 0.92, 0.97)+(0.93, 0.98, 1.00, 1.00)\big] \\
&= (0.321, 0.397, 0.555, 0.651)
\end{aligned}$$

In the same way,

$$\begin{aligned}
\tilde{R}_{C_2} &= \left[\mathrm{VH}\times\mathrm{L}+\mathrm{VH}\times\mathrm{H}+\mathrm{FH}\times\mathrm{FL}+\mathrm{H}\times\mathrm{L}+\mathrm{FH}\times\mathrm{H}+\mathrm{FH}\times\mathrm{H}\right]/\left[\mathrm{VH}+\mathrm{VH}+\mathrm{FH}+\mathrm{H}+\mathrm{FH}+\mathrm{FH}\right] \\
&= (0.301, 0.388, 0.654, 0.799)
\end{aligned}$$

$$\tilde{R}_{C_3} = [\text{VH} \times \text{H} + \text{FH} \times \text{FL} + \text{FH} \times \text{H} + \text{VH} \times \text{FH} + \text{AH} \times \text{FL}] / [\text{VH} + \text{FH} + \text{FH} + \text{VH} + \text{FH}]$$
$$= (0.402, 0.485, 0.736, 0.857)$$

$$\tilde{R}_{C_4} = [\text{VH} \times \text{H} + \text{FH} \times \text{H} + \text{VH} \times \text{FH}] / [\text{VH} + \text{FH} + \text{VH}]$$
$$= (0.510, 0.599, 0.861, 1.000)$$

$$\tilde{R}_{C_5} = [\text{VH} \times \text{FH} + \text{FH} \times \text{FH} + \text{AH} \times \text{FL} + \text{VH} \times \text{FH}] / [\text{VH} + \text{FH} + \text{FH} + \text{VH}]$$
$$= (0.486, 0.577, 0.854, 1.000)$$

$$\tilde{R}_{C_6} = [\text{FH} \times \text{H} + \text{FH} \times \text{FH} + \text{VH} \times \text{FH}] / [\text{FH} + \text{FH} + \text{VH}]$$
$$= (0.408, 0.497, 0.834, 1.000)$$

(3) **Calculating the risk rating —** By applying quantitative method of Eq. (10), the risk rating of $\tilde{R}_{C_1}$ is

$$f(\tilde{R}_{C_1}) = \int_0^1 \left| 2\tilde{\text{A}}(x) - 1 \right|$$
$$= \int_0^{0.321} dx + \int_{0.321}^{0.397} (26.2467x - 9.4304)\,dx$$
$$\int_{0.397}^{0.555} dx + \int_{0.555}^{0.651} (12.6661 - 21.0084x)\,dx + \int_{0.651}^{1} dx$$
$$= 0.924$$

In the same way,

$$f(\tilde{R}_{C_2}) = 0.884$$
$$f(\tilde{R}_{C_3}) = 0.897$$
$$f(\tilde{R}_{C_4}) = 0.882$$
$$f(\tilde{R}_{C_5}) = 0.906$$
$$f(\tilde{R}_{C_6}) = 0.873$$

(4) **Constructing the judge matrixes —** After calculating the risk ratings, each risk rating of attack types should execute multiplication to generate judge matrixes. From the rules of B_1,B_2, and B_3, the judge matrixes R_p, R_i, and R_u can be computed according to Table 8, Table 9 and Table 10. They are:

$$R_p = \begin{bmatrix} 0.000, & 0.000, & 0.000, & 0.366, & 0.274, & 0.183, & 0.091 \\ 0.000, & 0.000, & 0.000, & 0.088, & 0.177, & 0.354, & 0.265 \\ 0.000, & 0.000, & 0.000, & 0.000, & 0.449, & 0.359, & 0.090 \\ 0.000, & 0.000, & 0.000, & 0.000, & 0.088, & 0.441, & 0.353 \\ 0.000, & 0.000, & 0.000, & 0.000, & 0.091, & 0.362, & 0.453 \\ 0.087, & 0.087, & 0.087, & 0.175, & 0.262, & 0.175, & 0.000 \end{bmatrix} \quad R_i = \begin{bmatrix} 0.000, & 0.274, & 0.366, & 0.274, & 0.000 \\ 0.088, & 0.088, & 0.088, & 0.265, & 0.354 \\ 0.090, & 0.000, & 0.359, & 0.269, & 0.179 \\ 0.000, & 0.000, & 0.088, & 0.176, & 0.617 \\ 0.000, & 0.000, & 0.000, & 0.362, & 0.544 \\ 0.000, & 0.087, & 0.175, & 0.437, & 0.175 \end{bmatrix}$$

$$R_u = \begin{bmatrix} 0.000, & 0.366, & 0.548 \\ 0.265, & 0.442, & 0.177 \\ 0.538, & 0.359, & 0.000 \\ 0.088, & 0.265, & 0.529 \\ 0.091, & 0.362, & 0.453 \\ 0.437, & 0.437, & 0.000 \end{bmatrix}$$

Where each row means an attack type we defined in Fig. 5, and each column means a risk factor of the rules we defined from Table 7.

(5) **Calculating the quantitative coefficients and normalized weights —** From Table 8, the entropies of attack types of R_p can be calculated by applying Eq. (13), as follows:

$$e_{p_1} = -1/\ln 7 \ (0.4\ln 0.4+0.3\ln 0.3+0.2\ln 0.2+0.1\ln 0.1)=0.658$$

$$e_{p_2} = -1/\ln 7 \ (0.1\ln 0.1+0.2\ln 0.2+0.4\ln 0.4+0.3\ln 0.3)=0.658$$

$$e_{p_3} = -1/\ln 7 \ (0.5\ln 0.5+0.4\ln 0.4+0.1\ln 0.1)=0.485$$

$$e_{p_4} = -1/\ln 7 \ (0.1\ln 0.1+0.5\ln 0.5+0.4\ln 0.4)=0.485$$

$$e_{p_5} = -1/\ln 7 \ (0.091\ln 0.091+0.362\ln 0.362+0.453\ln 0.453)=0.485$$

$$e_{p_6} = -1/\ln 7 \ (3\times(0.1\ln 0.1)+2\times(0.2\ln 0.2)+0.3\ln 0.3)=0.871$$

Therefore, the vector of e_p can be described as:

$$e_p = (0.658,\ 0.658,\ 0.485,\ 0.485,\ 0.485,\ 0.871)$$

In the same way, the entropies of e_i, and e_u can be figured out as:

$$e_i = (0.677,\ 0.881,\ 0.795,\ 0.498,\ 0.418,\ 0.758)$$

$$e_u = (0.613,\ 0.936,\ 0.613,\ 0.817,\ 0.858,\ 0.631)$$

Then the weight vectors of attack types of each rule can be calculated by the Eqs. (12) and (14):

q_p = (0.145, 0.145, 0.219, 0.219, 0.219, 0.055)

q_i = (0.164, 0.061, 0.104, 0.254, 0.295, 0.123)

q_u = (0.253, 0.042, 0.253, 0.122, 0.093 0.241)

(6) **Calculating the total risk value —** From Table 8 to Table 10, we can get the weight vectors of risk factors, that is,

$B_p = (1/49,\ 3/49,\ 5/49,\ 7/49,\ 9/49,\ 11/49,\ 13/49)$

$B_i = (1/25,\ 3/25,\ 5/25,\ 7/25,\ 9/25)$

$B_u = (1/9,\ 3/9,\ 5/9)$

By applying Eq. (5), the risk value of each rule is calculates as follows:

$p_s = q_p R_p B_p^T = 0.199$

$c_s = q_i R_i B_i^T = 0.256$

$u_s = q_u R_u B_u^T = 0.295$

Finally, the total risk value between the AP1 and STA1 can be calculated by the Eq. (3)

$R = p_s + c_s + u_s - p_s c_s - p_s u_s - c_s u_s - p_s c_s u_s$

$=0.580$

4.1.5 Generating Attack Graph

Table 19. Risk Level of Total Risk Value

Total risk value (R)	Risk level
$0 \le R < 0.3$	Low (L)
$0.3 \le R < 0.43$	Fair low (FL)
$0.43 \le R < 0.57$	Medium (M)
$0.57 \le R < 0.7$	Fair high (FH)
$R > 0.7$	High (H)

According to the total risk value, we defined the risk levels, shown in Table 19, to express the risk level of the wireless environment. In order to clearly represent the risk value

between the AP and the station via attack graph, the connection relation, risk value, and risk level can be represented by a risk set. The risk set consists of four elements which are denoted as (AP_device, STA_device, Rsk_value, Rsk_level). AP_device represents an access point which is connected with a wireless station. STA_device represents a wireless station which connectes to an access point. Rsk_value represents the total risk value between the access point and the station. Rsk_level is regarded as the danger between two wireless devices according to Table 19. Therefore, graph drawing can be performed via Graphviz [25] and shown in Fig. 8 where the nodes and the edges are the wireless devices and the risk set between two devices, respectively.

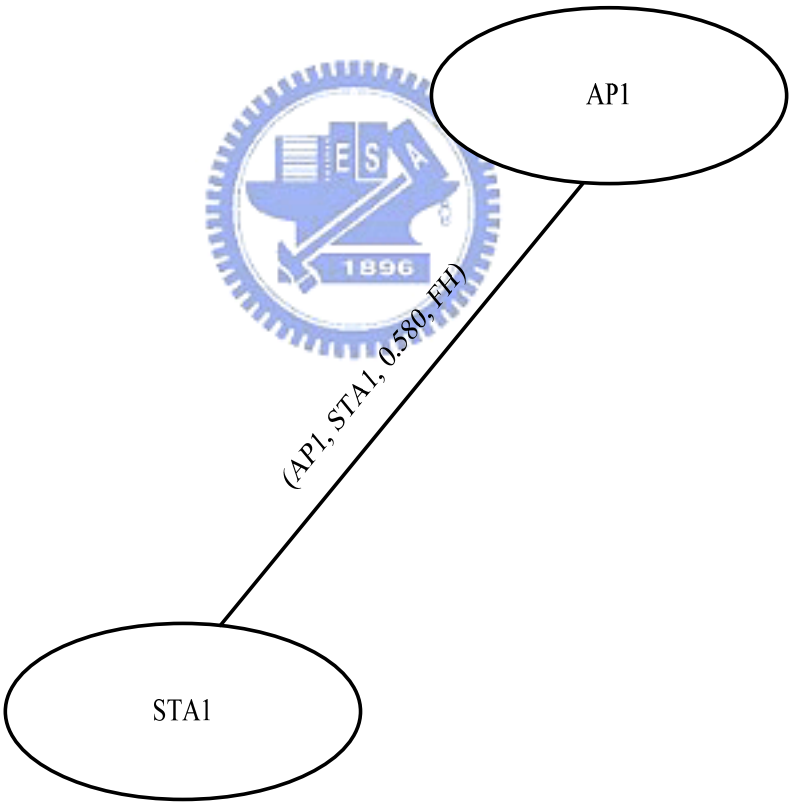


Fig. 8. Attack Graph with AP1 and STA1

4.2 Calculating Risk Value between Two Wireless Stations

After calculating risk value between an AP and a station from section 4.1, we can further

extend the analysis method to analyze the risk level between two stations. In this section, an extended environment of wireless network will be introduced for risk assessment.

4.2.1 The Environment of Wireless Network

Let us consider an environment of wireless network shown in Fig. 9, where the AP1 consists of two wireless stations STA1, STA2, and we want to analyze the risk between STA1 and STA2. Then the total risk value can be calculated via the configurations of the three wireless devices.

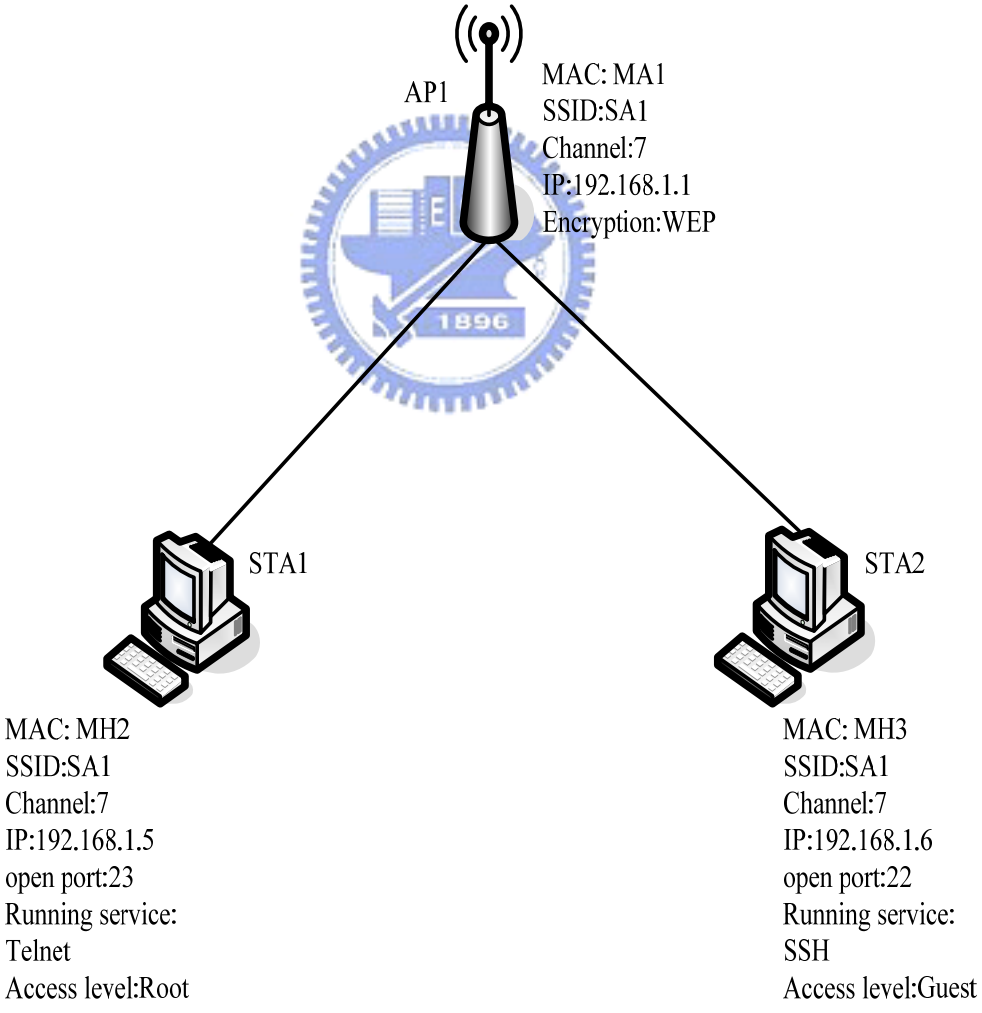


Fig. 9. Wireless Network Example (AP and two stations)

4.2.2 Determination of the Analysis Rules

The experts use the same rules to analyze a uniform assessable affair although they know that the analysis rules can be changed at any time. Once the rules are changed, the result of assessment will not be fair and objective. In order to equitably analyze the security of the wireless network, we should use the same criteria. Therefore, in this subsection, we use the same analysis rules from section 4.1.2 to analyze the wireless environment.

4.2.3 Algorithm

Because we use the same analysis rules, we should use the same algorithms to calculate the total risk value. In this example, all arguments are the same, expect the configuration file. From Fig. 9, we can generate three configuration files among AP1, STA1, and STA2. If we want to calculate the total risk value between AP1 and STA1, the configuration file should include 10 configurations consisted of AP1 and STA1. In the same way, the second configuration file includes 10 configurations comprised AP1 and STA2 in order to calculate the total risk value between them. As for the third configuration file, it is used to calculate the total risk value between STA1 and STA2. The configurations of the three wireless devices should be considered. Therefore, the third configuration file should contain 15 configurations. After obtaining the configuration files, the algorithm 4.2 can be used first to get the weight of each configuration, and then used algorithm 4.1 to obtain the total risk value among three wireless devices.

4.2.4 Evaluation

As former evaluation, we can obtain the total risk value between an AP and a wireless station. Thus, we do not calculate again. From Fig. 9, there are two connections, one is from AP1 to STA1, and the other is from AP1 to STA2. The result of assessment between AP1 and STA1 is 0.580, and the other result is 0.567. In the following, we use the proposed risk

assessment method to calculate the total risk value between STA1 and STA2. The procedures are decomposed as follows:

(1) **Constructing the security list table —** According to the configurations of Fig. 9, we can construct a linguistic security lists which includes the weights and risk levels of the configurations base on Table 12, Table 13, Table 16, and Table 17, as shown in Table 20.

Table 20. Linguistic List of the Weight and the Risk Level (AP1, STA1 and STA2)

Configuration		Attack type						Risk level
		C_1	C_2	C_3	C_4	C_5	C_6	
AP1	D_1	VH	VH					L
	D_2	VH	VH	VH	VH			H
	D_3		FH	FH				FL
	D_4	H	H					L
	D_5		FH		FH		FH	H
STA1	D_6		FH	FH				H
	D_7	VH		VH	VH	VH		FH
	D_8					FH	FH	FH
	D_9			AH		AH		FL
	D_{10}					VH	VH	FH
STA2	D_6		FH	FH				H
	D_7	VH		VH	VH	VH		FH
	D_8					FH	FH	FH
	D_9			AL		AL		FL
	D_{10}					M	M	FH

(2) **Calculating the fuzzy average set —** By using FWA method and fuzzy arithmetic operation from Eqs. (6) to (9), we can obtain the average fuzzy set of each attack type:

$$\tilde{R}_{C_1} = [\mathrm{VH} \times \mathrm{L} + \mathrm{VH} \times \mathrm{H} + \mathrm{H} \times \mathrm{L} + \mathrm{VH} \times \mathrm{FH} + \mathrm{VH} \times \mathrm{FH}] / [\mathrm{VH} + \mathrm{VH} + \mathrm{H} + \mathrm{VH} + \mathrm{VH}]$$

$$= [\ (0.93, 0.98, 1.00, 1.00) \times (0.04, 0.10, 0.18, 0.23)$$
$$+ (0.93, 0.98, 1.00, 1.00) \times (0.72, 0.78, 0.92, 0.97)$$
$$+ (0.72, 0.78, 0.92, 0.97) \times (0.04, 0.10, 0.18, 0.22)$$
$$+ (0.93, 0.98, 1.00, 1.00) \times (0.58, 0.63, 0.80, 0.86)$$
$$+ (0.93, 0.98, 1.00, 1.00) \times (0.58, 0.63, 0.80, 0.86)]$$
$$/ [(0.93, 0.98, 1.00, 1.00) + (0.93, 0.98, 1.00, 1.00)$$
$$+ (0.72, 0.78, 0.92, 0.97) + (0.93, 0.98, 1.00, 1.00)$$
$$+ (0.93, 0.98, 1.00, 1.00)]$$
$$= (0.365, 0.442, 0.610, 0.708)$$

In the same way,

$$\tilde{R}_{C_2} = [\mathrm{VH} \times \mathrm{L} + \mathrm{VH} \times \mathrm{H} + \mathrm{FH} \times \mathrm{FL} + \mathrm{H} \times \mathrm{L} + \mathrm{FH} \times \mathrm{H} + \mathrm{FH} \times \mathrm{H} + \mathrm{FH} \times \mathrm{H}]$$
$$/ [\mathrm{VH} + \mathrm{VH} + \mathrm{FH} + \mathrm{H} + \mathrm{FH} + \mathrm{FH} + \mathrm{FH}]$$
$$= (0.326, 0.417, 0.715, 0.875)$$

$$\tilde{R}_{C_3} = [\mathrm{VH} \times \mathrm{H} + \mathrm{FH} \times \mathrm{FL} + \mathrm{FH} \times \mathrm{H} + \mathrm{VH} \times \mathrm{FH} + \mathrm{AH} \times \mathrm{FL} + \mathrm{FH} \times \mathrm{H} + \mathrm{VH} \times \mathrm{FH} + \mathrm{AL} \times \mathrm{FL}]$$
$$/ [\mathrm{VH} + \mathrm{FH} + \mathrm{FH} + \mathrm{VH} + \mathrm{AH} + \mathrm{FH} + \mathrm{VH} + \mathrm{AL}]$$
$$= (0.426, 0.523, 0.835, 1.000)$$

$$\tilde{R}_{C_4} = [\mathrm{VH} \times \mathrm{H} + \mathrm{FH} \times \mathrm{H} + \mathrm{VH} \times \mathrm{FH} + \mathrm{VH} \times \mathrm{FH}] / [\mathrm{VH} + \mathrm{FH} + \mathrm{VH} + \mathrm{VH}]$$
$$= (0.510, 0.599, 0.861, 1.000)$$

$$\tilde{R}_{C_5} = [\mathrm{VH} \times \mathrm{FH} + \mathrm{FH} \times \mathrm{FH} + \mathrm{AH} \times \mathrm{FL} + \mathrm{VH} \times \mathrm{FH} + \mathrm{VH} \times \mathrm{FH} + \mathrm{FH} \times \mathrm{FH} + \mathrm{AL} \times \mathrm{FL} + \mathrm{M} \times \mathrm{FH}]$$
$$/ [\mathrm{VH} + \mathrm{FH} + \mathrm{AH} + \mathrm{VH} + \mathrm{VH} + \mathrm{FH} + \mathrm{AL} + \mathrm{M}]$$
$$= (0.331, 0.427, 0.784, 1.000)$$

$$\tilde{R}_{C_6} = [\mathrm{FH} \times \mathrm{H} + \mathrm{FH} \times \mathrm{FH} + \mathrm{VH} \times \mathrm{FH} + \mathrm{FH} \times \mathrm{FH} + \mathrm{M} \times \mathrm{FH}] / [\mathrm{FH} + \mathrm{FH} + \mathrm{VH} + \mathrm{FH} + \mathrm{M}]$$
$$= (0.261, 0.351, 0.753, 1.000)$$

(3) **Calculating the risk rating —** By applying quantitative method of Eq. (10), the risk rating of $\tilde{R}_{C_1}$ is

$$
\begin{aligned}
f\left(\tilde{R}_{C_1}\right) &= \int_0^1 \left|2\tilde{\mathrm{A}}(x)-1\right| \\
&= \int_0^{0.365} dx + \int_{0.365}^{0.442} (26.2467x - 9.4304)\,dx \\
&\quad \int_{0.442}^{0.610} dx + \int_{0.610}^{0.708} (12.6661 - 21.0084x)\,dx + \int_{0.708}^{1} dx \\
&= 0.904
\end{aligned}
$$

In the same way,

$$f\left(\tilde{R}_{C_2}\right) = 0.873$$

$$f\left(\tilde{R}_{C_3}\right) = 0.862$$

$$f\left(\tilde{R}_{C_4}\right) = 0.871$$

$$f\left(\tilde{R}_{C_5}\right) = 0.815$$

$$f\left(\tilde{R}_{C_6}\right) = 0.758$$

(4) **Constructing judge matrixes —** After calculating the risk ratings, each risk rating of attack types should execute multiplication to generate judge matrixes. From the rules of B_1, B_2, and B_3, the judge matrixes R_p, R_i, and R_u can be computed according to Table 8, Table 9, and Table 10. They are:

$$R_p = \begin{bmatrix}
0.000, & 0.000, & 0.000, & 0.364, & 0.273, & 0.182, & 0.091 \\
0.000, & 0.000, & 0.000, & 0.087, & 0.174, & 0.348, & 0.261 \\
0.000, & 0.000, & 0.000, & 0.000, & 0.431, & 0.345, & 0.086 \\
0.000, & 0.000, & 0.000, & 0.000, & 0.087, & 0.435 & 0.349 \\
0.000, & 0.000, & 0.000, & 0.000, & 0.081, & 0.326, & 0.408 \\
0.076, & 0.076, & 0.076, & 0.151, & 0.227, & 0.151, & 0.000
\end{bmatrix}$$

$$R_i = \begin{bmatrix}
0.000, & 0.273, & 0.364, & 0.273, & 0.000 \\
0.087, & 0.087, & 0.087, & 0.262, & 0.349 \\
0.086, & 0.000, & 0.345, & 0.258, & 0.173 \\
0.000, & 0.000, & 0.087, & 0.174, & 0.610 \\
0.000, & 0.000, & 0.000, & 0.326, & 0.489 \\
0.000, & 0.075, & 0.151, & 0.378, & 0.151
\end{bmatrix}$$

$$R_u = \begin{bmatrix}
0.000, & 0.364, & 0.546 \\
0.261, & 0.436, & 0.174 \\
0.518, & 0.345, & 0.000 \\
0.087, & 0.261, & 0.523 \\
0.081, & 0.326, & 0.408 \\
0.379, & 0.379, & 0.000
\end{bmatrix}$$

(5) **Calculating the quantitative coefficients and normalized weights —** From Example 1, the entropies of attack types of R_p, R_i, and R_u have been calculated by applying Eq. (13), they are:

$$e_p = (0.658,\ 0.658,\ 0.485,\ 0.485,\ 0.485,\ 0.871)$$

e_i = (0.677, 0.881, 0.795, 0.498, 0.418, 0.758)

e_u = (0.613, 0.936, 0.613, 0.817, 0.858, 0.631)

In the same way, the weight vectors of attack types of each rule can be calculated by the Eqs. (12) and (14):

q_p = (0.145, 0.145, 0.219, 0.219, 0.219, 0.055)

q_i = (0.164, 0.061, 0.104, 0.254, 0.295, 0.123)

q_u = (0.253, 0.042, 0.253, 0.122, 0.093 0.241)

(6) **Calculating the total risk value —** By applying Eq. (2), the risk value of each rule is calculates as follows:

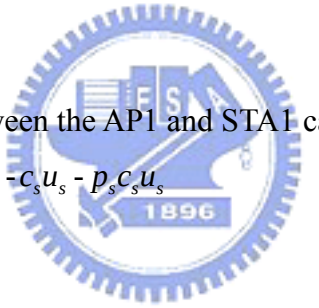
$$p_s = q_p R_p B_p^T = 0.186$$

$$c_s = q_i R_i B_i^T = 0.241$$

$$u_s = q_u R_u B_u^T = 0.282$$

Finally, the total risk value between the AP1 and STA1 can be calculated by the Eq. (3)

$$R = p_s + c_s + u_s - p_s c_s - p_s u_s - c_s u_s - p_s c_s u_s$$
$$= 0.556$$



4.2.5 Generating Attack Graph

In order to clearly represent the risk value between the two wireless stations via attack graph, the risk set can be redefined and represented as (Src_device, Dst_device, Rsk_value, Rsk_level). Src_device represents source station. Dst_device represents destination station. Rsk_value and Rsk_level have illustrated above. Therefore, graph drawing can be performed via Graphviz [25] to represent the risk values among three wireless devices, as shown in Fig. 10.

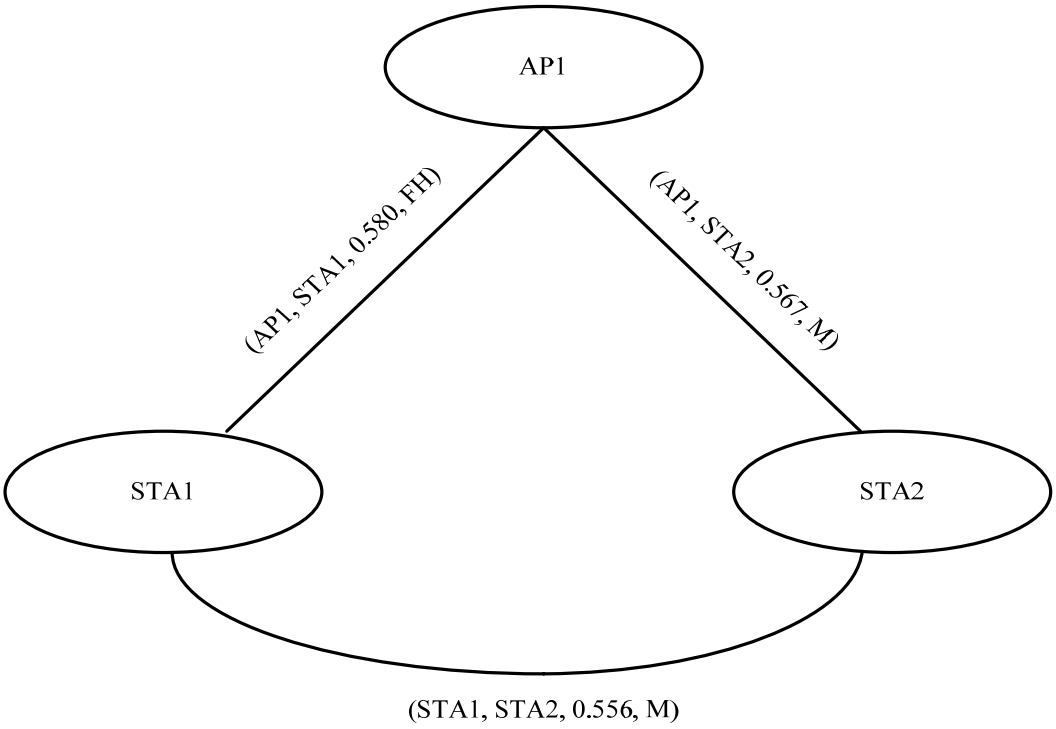


Fig. 10. Attack Graph with AP1, STA1 and STA2

4.3 Summary

From Examples 4.1and 4.2, it is obvious that our method can used in wireless risk assessment, and then we can obtain the quantitative value from the average fuzzy set. It overcomes the shortcomings of the traditional fuzzy linguistic measure method which are presented in [32], [33] and [34]. Furthermore, if we use the attack graph for describing the wireless environment, then it can help the administrator to obtain more detailed information of wireless environment and avoid being attacked by attackers.

Chapter 5
Conclusion and Future work

In this thesis, we have proposed a new model for risk assessment based on the fuzzy linguistic measure method and AHP method. First, we design a hierarchy architecture which considers the configurations that attackers will use to launch the attack for wireless risk assessment. It is more flexible than the exiting architectures because some configurations will be changed by the users. Thus the administrators can revise total risk value dynamically. Also, some operations are defined in order to obtain the quantitative value of fuzzy set. It is usable for administrators to do sensitivity analysis on the selected fuzzy set. In addition, this method is combined with the AHP method. It really help administrators to obtain the risk value objectively based on the expert experience. Finally, we generate attack graph according to actual wireless environment. The graph helps administrators not only understand the risk value between two wireless devices but also support them to enhance the security robustness of the wireless environment.

In the future, more analysis rules should be designed to make the result of assessment more precise. Besides, the process is needed to deal with conflicting interests in the judge matrix for risk assessment. This is relevant to the situation where autonomous experts with incomplete information need to make a group decision.

References

[1] M. Borse and H. Shinde, "Wireless Security & Privacy," *IEEE International Conference on Personal Wireless Communications*, ICPWC, pp. 424-425, January 2005.

[2] W. A. Arbaugh, N. Shankar and Y.C. Justin, "Your 802.11 Wireless Network has No Clothes," pp. 1-13, March 2001. [Online]. Available: http://www.cs.umd.edu/~waa/wireless.pdf

[3] G. Lehembre, "Wi-Fi Security – WEP and WPA," pp. 2-15, June 2005. [Online]. Available: http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf

[4] D. Welch and S. Lathrop, "Wireless Security Threat Taxonomy," *In proc. of IEEE Workshop on Information Assurance United States Military Academy*, West Point, pp.76-83, June 2003.

[5] L. A. Mohammed and B. Issac, "DoS Attack and Defense Mechanisms in Wireless Network," *IEEE International Conference on Mobile Technology*, Application and System, pp. 1-8, November 2005.

[6] F. Lau, S. H. Rubin, M. H. Smith and L. Trajkovic, "Distributed Denial of Service Attacks," *IEEE International Conference on System, Man*, Cybernetics, Vol. 3, pp. 2275-2280, October 2000.

[7] Q. Huang, H. Kobayashi and B. Lin, "Modeling of Distributed Denial of Service Attacks in Wireless Network," *IEEE Pacific Rim Conference on Communication, Computer and signal Processing*, PACRIM, Vol. 1, pp. 41-44, August 2003.

[8] O. Sheyner, J. Haines, S. Jha, R. Lippmann and J. M. Wing, "Automated Generation and Analysis of Attack Graph," *In Proc. of IEEE Symposium on Security and Privacy*, pp. 273-284, May 2002.

[9] R. Ortalo, Y. Deswarte and M. Kaaniche, "Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security," *IEEE Transactions on Software Engineer*, Vol. 25, No. 5, pp. 633-650, October 1999.

[10] C. Phillips and L. P. Swiler, "A Graph-Based System for Network Vulnerability Analysis," *In Proc. of the workshop on New security paradigms NSPW '99 Publisher*, pp. 71-79, January 1999.

[11] L. P. Swiler, C. Phillips, D. Ellis and S. Chakerian, "Computer-Attack Graph Generation Tool," *In Proc. of DARPA Information Survivability Conference & Exposition II*, Vol. 2, pp. 307-321, June 2001.

[12] P. Ammann, D. Wijesekera and S. Kaushik, "Scalable, Graph-Based Network Vulnerability Analysis," *In Proc. of 9th ACM Conference on Computer and Communication Security*, Washington, pp. 217-224, November 2002.

[13] K. Ingols, R. Lippmann and K. Piwowarski, "Practical Attack Graph Generation for Network Defence," *In Proc. of the 22nd Annual Computer Security Applications Conference*, pp. 121-130, December 2006.

[14] T. Zhang, M. Z. Hu, D, Li and L. Sun, "An Effective Method To Generate Attack Graph," *In Proc. of the Fourth International Conference On Machine Learning and Cybernetics*, Guangzhou, pp. 3926-3931, August 2005.

[15] S. Noel, M. Jacobs, P. Kalapa and S. Jajodia, "Multiple Coordinated View for Network Attack Graph," *IEEE Workshop on Visualization for Computer Security*, pp. 99-106, October 2005.

[16] I. Koteko and M. Stepashkin, "Attack Graph Based Evaluation of Network Security," *In Proc. of IFIP International Federation for Information*, pp.216-227, 2006.

[17] B. Schneier, "Modeling Security Threats," Dr. Dobb's Journal, December 1999. [Online]. Available: http://www.schneier.com/paper-attacktrees-ddj-ft.html#rf3

[18] S. Jha and J. Wing, "Survivability Analysis of Network Systems," *In Proc. of the International Conference on Software Engineering*, Toronto, Canada, pp.1-20, May 2001.

[19] H. J. Schumacher, S. Ghosh, "A Fundamental Framework for Network Security," *Journal of Network and Computer Application*, Vol. 20, No.7, pp. 305-322, July 1997.

[20] E. W. T. Ngai and F. K. T. Wat, "Fuzzy Decision Support for Risk Analysis in E-commerce Development," *Decision Support Systems*, Vol. 40, No.2, pp. 235-255, March 2004.

[21] K. Clark, S. Tyree, J. Dawking and J. Hale, "Qualitative and Quantitative Analytical Techniques for Network Security Assessment," *in Proc. of IEEE Workshop on Information Assurance and Security*, West Point, NY, pp. 321-328, June 2004.

[22] T. R. Peltier, *Information Security Risk Analysis*. Boca Raton, FL :Auerbach, 2001.

[23] S.. Jha, O. Sheyner and J. M. Wing, "Minimization and Reliability Analyses of Attack Graph," *Computer Security Foundations Workshop*, Novia Scoria, Canada, June 2002.

[24] NuSMV, "NuSMV: A New Symbolic Model Checker," [Online]. Available: http://afrodite.itc.it:1024/nusmv/.

[25] Graphviz, "Graph Visualization Software," [Online]. Available: http://www.graphviz.org/

[26] S. Gray, G. Alice and F. Alexis, "Risk Management Guide for Information Technology System," *National Institute of Standards and Technology*, July 2002.

[27] D. M. Zhao, J. H. Wang, J. Wu and J. F. Ma, "Using Fuzzy Logic and Entropy Theory to Risk Assessment of the Information Security," *In Proc. of the Fourth International Conference on Machine Learning and Cybernetics*, Guangzhou, 18-21, pp. 2248-2253, August 2005.

[28] D. M. Zhao, J. H. Wang, J. Wu and J. F. Ma, "Fuzzy Risk Assessment of the Network Security," *In Proc. of the Fourth International Conference on Machine Learning and Cybernetics*, Guangzhou, 13-16 ,pp. 4400-4405, August 2006.

[29] S. H. Chen and C. L. Hwang, *Fuzzy Multiple Attribute Decision Making: Methods and Applications.* Springer Verlag, Berlin, Heidelberg, New York, 1992.

[30] A. Valishevsky, "Granular information based risk analysis in uncertain situation," *In Proc. of the 4th International Scientific and Practical Conference on Environment*, Rezekne, Latvia, pp. 385-391, June 2003.

[31] W. Changguang, Z. Dongmei, and M. Jianfeng, "A Risk Assessment Method of the Wireless Network Security," *Journal of Electronics*, Vol. 24, No.3, pp. 428-432, May 2007.

[32] R. Kangari and L. S. Riggs, "Construction Risk Assessment by Linguistics," *IEEE Transactions on Engineer Management*, Vol. 36, No.1, pp. 126-131, May 1989.

[33] S. J. Chen and S. M. Chen, "Fuzzy Risk Analysis Based on Similarity Measures of Generalized Fuzzy Numbers," *IEEE Transactions on Fuzzy Systems*, Vol. 11, No.1, pp. 45-56, February 2003.

[34] Y. Liao, C. Ma and C. Zhang, "A New Fuzzy Risk Assessment Method for Network Security Based on Fuzzy Similarity Measure," *In Proc. of the 6th World Congress on Intelligent Control and Automation*, WCICA 2006, pp 8486-8491, June 2006.

[35] G. Klir and B. Yuan, *Fuzzy Set and Fuzzy Logic: Theory and Application*, Prentice Hall, Singapore, pp. 275- 269, June 2005.

[36] C. L. Hwang and K. Yoon, *Multiple Attribute Decision Making: Methods and Applications.* Springer Verlag, Berlin, Heidelberg, New York, pp. 41-57, 1981.

[37] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, December 1999.