Risk Surveillance Control of Wireless Security Attack with Fuzzy Rules

Dr. Abdulkareeem Merhej Radhi

Assistant Professor, Al-Nahrain University, Information Engineering College, Baghdad-Iraq

Abstract: ***Due to the rapid development of software's and algorithms that attack wireless connections, as well as risky challenges which encounter the data passing through this connection with the development of the potential capabilities of intruders, urgent manage risks of this wireless connections arises which it became necessary to analysis and protect this data. This paper propose a compromising way between protecting data from eavesdropping with intruding and risks. The paper introduces a new type of cryptographic algorithm that minimize these risks. The proposed rules that process these risks adopted on fuzzy theory. The target packets captured for local area network using WIRESSHARK free source software, then tested, and results discussed which concludes that minimizing risk for this network in diagnosed cases can be achieved via controlling transmitted data via the proposed encryption system. Matlab Guide toolbox 2013 and Laptop with Intel processor I5 with RAM 8GB was used.***

Keywords: Risk, Cryptography, Fuzzy, Packets, WLAN

1. Introduction

Wireless networking presents many advantages productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interceptions greater than with wired networks. If the message not encrypted, or encrypted with a weak algorithm, the attacker can read it, there by compromising confidentiality. Although wireless networking alters the risk associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems.Sothe aim is to control wireless security attacks and manage risk with different probabilities to made decisions according to each case [1].

Wireless networks generate large amount of data, which often is sensitive and vulnerable to interceptions than wired networks. This has increased the risk for users significantly and to combat this consideration, wireless networks users may choose to utilize various encryption methodologies. Encryption is the key to keep information secure online in a Wi-Fi network. When information is encrypted, it is scrambled into a code so others can't get it. Thus, due to the high probability of information compromise associated with Wi-Fi networks, various encryption methods have been developed. However, commonly utilized encryption methods are known to have weaknesses and are susceptible to attackers thereby compromising confidentiality [2].

2. Paper Outline

The rest of this paper structured as follows: Section 3, offers the main aim and contributions of this research while Section 4, presents WLAN Vulnerabilities. Section 5 discuss overview of the general attacks and Section 6 introduce how to securing A Wireless LAN. Section 7, related works and literatures review are presented. While Sections 8,9 and 10, discusses the fundamentals and foundations of the adapted of the proposed method and its methodology.

3. Aims and Contribution

Due to the use of wireless telecommunications networks at the present time and the huge of data passing through it besides the importance and confidentiality of data became very important to discover of modern and new ways to protect it against various types of attacks and penetration. Proposed research is a new way to protect data from unsecure and illegal threats of all kinds, which have been discussed in next sections. From the view point of the researcher, the encryption of data transmitted over wireless channels considered as the easiest and a way to protect data and it can be a maximum safety mean such that it can operate according to different circumstances in spite of how many ways evolved penetration.

4. WLAN Vulnerabilities

Wireless LANs have gained much more popularity than wired networks because of their flexibility, cost-effectiveness and ease of installation. However, the increasing deployment of WLANs presents the hacker or cracker with more opportunities. Unlike wired networks, WLANs transmit data through the air using radio frequency transmission or infrared. Current wireless technology in use enables an attacker to monitor a wireless network and in the worst case may affect the integrity of the data. There are a number of security issues that presents the IT security practitioner, system administrator securing the WLAN with difficulties [3].

As the name implies Wired Equivalent Privacy (WEP) was intended to provide users with the same level of privacy as that of a wired LAN. However, when this protocol was first developed by the IEEE 802.11b Task Force in 1999, it quickly proved to be less secure than its wired equivalent. WEP comes as 64 bit or 128 bit but the actual transmission keys are 40 bits and 104 bits long. In each case the other 24 bits is an Initialization Vector (IV). Before transmission, the packets are encrypted with a symmetric encryption algorithm (RC4) using a session key which is made up of the IV and the default transmit key. The IV is randomly generated for each session but the default transmit key is fixed. The IV is sent in the packet along with the data. Once the encrypted packet reaches the receiving end, it decrypts the packet using the same session key [4].

However, WEP has some serious security problems. It fails to meet the fundamental security goals of confidentiality, integrity and authentication. The main problem with WEP is that the 40 or 104 bit keys are static and common to all users in the WLAN. Since, WEP does not provide an effective key management technique, changing the keys on all devices is a time consuming and difficult task. Thus, if any devices are lost or stolen, the higher the chances of the key being compromised. More importantly, the encryption algorithm RC4 used in WEP is flawed and encryption keys can be recovered through cryptanalysis. Besides the default transmission key, the IV is short and can be easily sniffed by passive attack using freely available software tools. One of the other problems is that WEP is disabled by default and its use is optional, therefore, many users never turn on encryption. It is better to use of some form of encryption than no encryption at all.

5. Overview of General Attacks

An attack is an action that is carried out by an intruder in order to compromise information in an organization. Unlike wired networks, a WLAN uses radio frequency or infrared transmission technology for communication; thus, making them susceptible to attack. These attacks are aimed at breaking the confidentiality and integrity of information and network availability. Attacks are classified into the following two categories [1] :

- Passive attacks.
- Active attacks

Passive attacks are those types of attack in which the attacker tries to obtain the information that is being transmitted or received by the network. These types of attacks are usually very difficult to detect as there is no modification of the contents by the attacker . There are two types of passive attack and these are traffic analysis and eaves dropping.

On the other hand, active attacks where the attacker not only gains access to the information on the network but also changes the information contents or may even generate fraudulent information on the network. This type of malicious act, results in great loss for any organization. Following are a list of active attacks in WLAN technology:

- Unauthorized Access
- Rogue Access Point
- Man in the Middle Attack (MITM)
- Denial-of-Service
- Reply Attack
- Session High jacking

According to the CIA triad, information security should meet three main principles, which are confidentiality, integrity and availability. All three concepts are needed to some extent to achieve true security. Otherwise, the network will be vulnerable to attack. Furthermore, two other principals involved i.e. access control and authentication.Based on the CIA triad, access control and the authentication definitions described, various types of attack/threats in a WLAN are discussed below. These attack categories can also fall in the above active or passive types.

6. Securing A Wireless LAN

The above vulnerabilities and threats come to the conclusion that it is very important to make sure that the wireless network is secure whether for a home user or an enterprise network. However, still there is no true security solution that has been implemented and is presently available. Virtual Local Area Networks (VLAN) are another technology that can be used in corporate wireless network to enforce a security policy. VLANs work by tagging LAN frames assigned to different workgroups. Those tags actually decide where incoming frames can and cannot go within the corporate network. For example, if a business provides guest and consultant access, all traffic coming from that wireless LAN will be tagged so that traffic is limited to the public internet thus, keeping them away from corporate data and services [1].

A wireless intrusion detection and prevention system can be an essential tool for identifying intrusions and notifying the system administrator of attacks. There is no option to stop passive sniffing on the network with the traditional firewall. As a result, WIDS/WIPS can be deployed to act as a watchdog in order to detect and prevent new threats and any malicious activity. A VPN used with WIDS/WIPS can provide a good security measure by actively monitoring the network to identify anomalies. This adds another layer of assurance for data confidentiality [1].

Security configurations and are always compliant with the organization’s security policies. Furthermore, the organization should implement continuous attack and vulnerability monitoring and perform periodic technical security assessment to measure overall security of the WLAN [5]. The use of strong encryption standards protect WLANs from the worst threats. The best practice would be to enable Wi-Fi protected access WPA/WPA2 rather than WEP[6].

7. Related Works

To minimize the chances of software project failure need to proper study all the risk factors which can have direct or indirect effect on the success of software product. Much application development used to make the software in efficient manner and various steps each risk defined. Tools are available for management of various kinds of risks. Fuzzy logic approach used to identify threats for the risks. This logic composed of fuzzy sets, provides the concept of degrees of membership, which increases the number of possibilities that can be subject to research. This logic is perfect deal with uncertain risk come in project management [2].

Bhatia and sumbaly[3] suggest Quantum cryptography to provides a solution towards absolute communication security over the network by encoding information as polarized photons, which can be sent through the air. Quantum cryptography is an evolving technology that provides safety and security for network communication by performing cryptographic tasks using quantum mechanical effects. Quantum Key Distribution (QKD) is a technique that is an application of quantum cryptography that has gained popularity recently since it overcomes the flaws of conventional cryptography. QKD makes the secure distribution of the key among different parties possible by using properties of physics. Research has shown that use of QKD to distribute network key raises the security and makes it harder for an eavesdropper to interrupt communication. With the proposed modification, this paper has achieved the main objective of improving security of WLANs.

Sedghi and Kaghazgaran introduce public key cryptography to secure wireless network security[8]. The use of Public key cryptography PKC in sensor networks has been usually considered as nearly impossible, but at present some studies [4] have started to consider the possibility of utilizing PKC in a highly-constrained networks. They conclude that authentication and key exchange protocols using optimized software implementations of public-key cryptography are very viable on small wireless devices.

He [4] analyze IEEE 802.11i with respect to data confidentiality, integrity, mutual authentication, and availability. Threat model, 802.11i appears to provide effective data confidentiality and integrity when CCMP is used. 802.11i may also provide satisfactory mutual authentication and key management, although there are some potential implementation oversights that may cause severe problems. On the other hand, He identified several Denial of Service attacks. Different solutions are proposed for these vulnerabilities, which result in an improved variant of 802.11i with a more efficient failure recovery mechanism. Some of the resulting improvements have been adopted by the IEEE 802.11 TGi in their final deliberation. He used a finite-state verification tool, called MurØ, to analyze the 4-Way Handshake component. The result shows that finite-state verification is quite effective for analyzing security protocols. Furthermore, He adopted Protocol Composition Logic to conduct a correctness proof of 802.11i, including SSL/TLS as a component. Finally, His research showed that 802.11i can significantly reduce the complexity of designing a secure routing protocol when it is deployed in wireless ad hoc networks.

8. Methodology

The proposed work is a new technique to protect passingdata via wireless networks from eavesdropping and illegal interceptors. The main aim for this technique is to manage and control transmission packets to minimize risks. Moreover, this technique assumes that the transmitted data was used as a tested data to achieve different attacks with several attack circumstances. Proposed intrusion detection system for this work detected the malicious activities and attacked through proposed system wall.

9. Intrusion Detection Technique

Unsupervised learning classifier was used to monitor network and detect malicious intruders. Flow Data collected then features extracted and analyzed. Figure (1) depict flow chart of this technique.

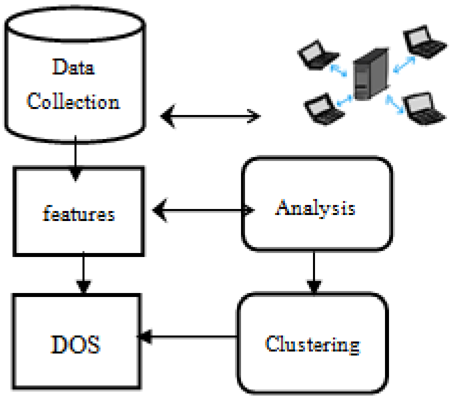


Figure [1]: Proposed IDS

In IDS packets features extracted using rule header:

***[Action][Protocol][SourceIP][Sourceport]->
[destIP][destport] ([Rule options])***

Compare contents for a series of packets indicate similar nearest value features, which are a good indicator to belonging to the same patterns. *Information gain of a term measures the number of bits of information obtained for category prediction by the presence or absence of the term in a document. Let m be the number of classes [6]. The information gain of a term t is defined as*

$$IG(t) = -\sum_{i=1}^{m} P(c_i) log P(c_i) + \\ +P(t)\sum_{i=1}^{m} P(c_i|t)\ log\ P(c_i|t) \ldots\ldots\ldots \textbf{(1)} \\ +P(\acute{t})\sum_{i=1}^{m} P(c_i|\acute{t})\ log\ P(c_i|\acute{t})$$

to measure the association between each cluster and a term χ^2used to define different clusters

$$\chi^2\ \mathbf{(t,c)}=\frac{N\times(p(t,c)\times P(\overline{\acute{t},\acute{c}})}{P(t)\times P(\acute{t})}-\frac{P(t,\acute{c})\times P(\acute{t},C))^2}{P(C)\times P(\acute{C})}\ldots\mathbf{(2)}$$

to classify packets (terms) in a category i , entropy with ascending ranking used in this classification, such that

(t) = -
$\sum_{i=1}^{N}\sum_{i=1}^{N}(S_{i,i} \times log\ (S_{i,i}) + (1 - S_{i,i}) \times log\ (1 - S_{i,i}))$ **(3)**

$$S_{i,j} = e^{-\alpha\times dist_{i,j}}, \alpha = -\frac{\ln(0.5)}{dist} \ldots\ \mathbf{(4)}$$

Where $dist_{i,j}$ is the distance between two packets i,j when deleting t.

9.1 Entropy

To check the performance of the obtained classifier that detect set of packets in a specific cluster, entropy measurement used as a tool for diagnosing a malicious attack. So, If a set of packets (M) belonging to a cluster

Entropy (impurity, disorder) of a set of examples, relative to a binary classification is -

$$\textit{Entropy}\ (M) = -p_+ \log_2 (p_+) - p_- \log_2 (p_-) \text{- -}\ \mathbf{(5.1)}$$

Where P_+ is the proportion of positive examples in (M) and P_- is the proportion of negatives. For multiple category problems with C categories, entropy can be generalized to:

$$\underline{Entropy\ (M)} = \sum_{I=1}^{C} - P_i \log_2 (P_i) \quad \text{---------} \ \mathbf{(5.2)}$$

Where P_i is the proportion of category i examples in M.

The information gain of an attribute is the expected as reduction in entropy caused by portioning on this attribute:

$$\underline{Gain\ (M, A)} = Entropy\ (M) - \sum_{v \in Values\ of\ A} \frac{}{|M|}\ Entropy(M_v) \ \ldots\ldots\ldots\mathbf{(5.3)}$$

Where $\underline{M_v}$ is the subset of M for which attribute A has value v and the entropy of the partitioned data calculated by weighting the entropy of each partition by its size relative to the original set.

9.2. Performance

Measured in terms of recall and precision, where recall is the percentage of positive instances that were formed by rule base.

Precision measures the percent correct of instances extracted by the rule base [12].

$$\mathbf{Recall} = \frac{\textit{Number of correctly predicted entities}}{\textit{Number of entities that should have been found}} \qquad (5.4)$$

$$\mathbf{Precision} = \frac{\textit{Number of correctly predicted entities}}{\textit{Number of all entities predicted}} \qquad (5.5)$$

9.3 Evaluation Method

The *F*-measure was used as the evaluation measure. For every classification, we can calculate

a = (the number of data the classifier evaluates positive for positive data),

b = (the number of data the classifier evaluates positive for negative data),

c = (the number of data the classifier evaluates negative for positive data).Then, we can calculate precision (*P*) and recall (*R*) as

$$P = \frac{a}{a+b} \ldots..(5.6)$$

$$R = \frac{a}{a+c} \quad \ldots.(5.7)$$

By combining precision and recall, the F-measure defined as follows:

$$F = \frac{1+\beta^2}{\frac{1}{P} + \beta^2 \frac{1}{R}} \quad \ldots\ldots\ \mathbf{(5.8)}$$

The F-measure varies between 0 and 1. The larger the F-measure becomes, the higher the classification accuracy gets. $\beta$is a weight parameter, and we set $\beta = 1$.

10. Fuzzy Logic and Fuzzy Rules

As a complement to probability models, fuzzy logic models can be applied to assess risks for which there is insufficient data and incomplete knowledge [7]. Fuzzy logic provides a framework where human reasoning and imprecise data can contribute to risk analysis. Inference rules in a fuzzy logic model may help not only to identify the cause of a certain risk but also to design efficient and effective mitigation plans.

Fuzzy logic systems assist us in building knowledge of risks in two ways:

1) The systems keep risk managers and subject matter experts free from the inference part for many risks and let them focus on cause-and-effect relationships based on their knowledge [7].
2) Risk assessment results flow into the risk decision-making process, and the outcomeof the decision can then be fed back into the system to refine the fuzzy sets, rules and understanding. Fuzzy logic models may be used with other risk models such as decision trees and artificial neural networks to model complicated risk issues like policyholder behaviors.

The proposed work is a new technique to protect passingdata via wireless networks from eavesdropping and illegal interceptors. The main aim for this technique is to manage and control transmission packets to minimize risks. Moreover, this technique assumes that the transmitted data was used as a tested data to achieve different attacks with several attack circumstances. Proposed intrusion detection system for this work detected the malicious activities and attacked through proposed system wall.

11. Minimizing Risk

After analyzing and studying all risk factors, the main challenge minimizing risk in wireless network security. So packets encryption should be tackled according to the types of attacks after analysis. Analysis of attack should be taken in order to the type of attack explained in section [5].

12. Fuzzy Inferences

Fuzzy logic operators can be used as the basis for inference systems. Such fuzzy inference methods have been extensively studied by the expert systems community. Knowledge that can be only formulated in a fuzzy, imprecise manner can be captured in rules that can be processed by a computer.

12.1 Inferences from Imprecise Data

Fuzzy data can be simulated as rules called inference rules. It has the same structure as crisp ones. For example the rules *G1*and *G2*, may have the form:

$$G_1\text{:If}(\neg A\ \tilde{}\wedge B)\ \text{then}\ G_3.$$
$$G_2\ \ \text{:If}(G_3 \vee B)\ \ \text{then}\ G_4.$$

the operands may assign numeric values .

12.2. Inference Rules with Risk Assessment and Decision Making

A key feature of fuzzy sets is that there are no hard rules about how their membership functions are defined [10]. In order to establish inference rules from fuzzy data in WLAN security system, independent and dependent variables must be selected and then fuzzy sets with numeric values adopted. In this research, robust and unbreakable data is dependent variables while true packets are independent variable.

13. Algorithm

Adopting this algorithm to achieve two important features for security of data transmitted over wireless networks, first, the reliability and second data security. Where it is in the first accrediting Hash algorithm via the sender's IP exploitation and recipient. To have higher security for the transmitted data, which are formed as a packets, we adopt the following algorithm:

1) The idea relies mainly on the basis of encryption packets sent over the air.
2) Shift Register was used for this purpose of a length of 16 numbered packets.
3) Initial key known only by the sender which represented by a Shift Register a 16-bit long only.
4) Also there is a primary key of length 64 bit represented by (four Shift Registers) each 16,bits long .
5) Also relying to another key which is a message key of length 16 bits.
6) Every single bit of the message key integrates with Shift Register output for the primary key, according to the following sequence nonlinear the function: $O_n = Bk_{o_n} \oplus MK_{o_n}$
7) All 16-bit per package integrates with outputs using XOR function.
8) On the other hand the recipient receive output data and open the encrypted packets and reverse cycle of the algorithm described in the previous points until the original package extracts the data.

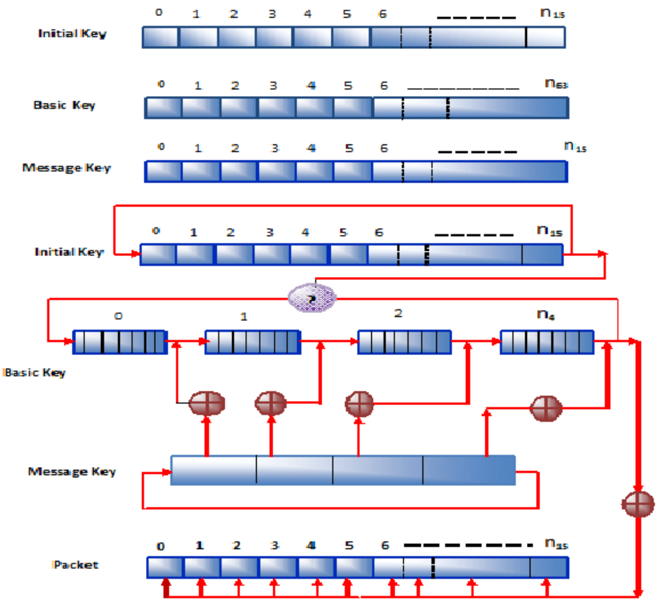


Figure 2: Proposed Encryption Algorithm

14. Rule Base

This paper adopts a fixed methodology in building system of rules that are control data sent and received and which contains fuzzy values. Where rules and axioms used to develop and conclude facts and rules with logical math. The modified rules are: modus ponens, modus tollens, addition, simplification, hypothetical syllogism, Disjunctive syllogism, and resolution. The following rules are seeds of inference rule base of the proposed system:

1) ("if risk then packets") is accepted, but the antecedent risk holds, then the consequent encryption cannot be activated.
2) ("if risk then packets") is accepted, but the consequent (packets) does not hold, then the negation of the antecedent encryption can be activated.
3) If ("risk and packets") is accepted but the consequent risk can be accepted then encryption cannot be activated..
4) If ("risk or packets") is accepted but the negation of antecedent (risk) holds then the encryption can be activated.
5) (" if risk then packets") is accepted, but the antecedent ("if risk then encryption") holds, then risk implies encryption can be activated.
6) If risk is accepted and the antecedent packets holds, then the consequent risk and encryption cannot be activated.

So we have compromising between accepted risks and number of packet values which are gained from practical tested proposed algorithm. The range of risk values between (0 to 4.5), while the range number of the accepted packets which is not affected by the type of attack technique explained in section 5 is (100 to 100000).

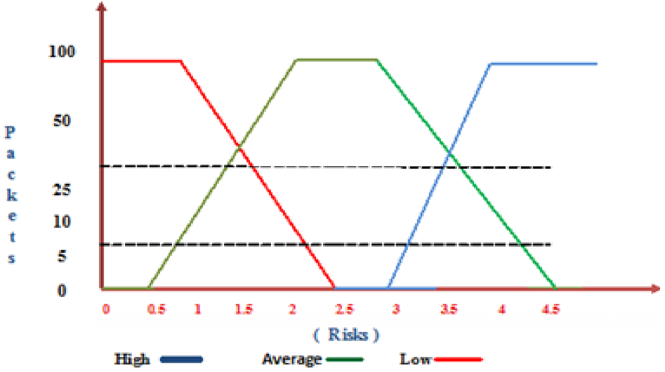


Figure 3- Surveillance Risk

15. Wireless software Infrastructure

Figure (4) presents software infrastructure, where network link ETHERENT with TCP/UDP protocol to capture packets and analyze it.

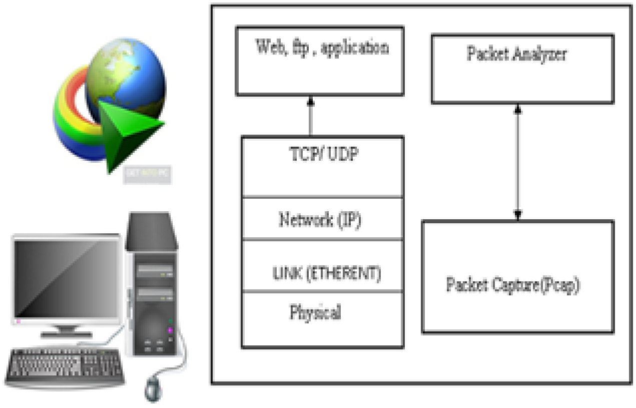


Figure [4]: Wireless Software Infra structure

16. Preparing Data

Capturing packets with protocols for the target network is the first step in preparing target data. Wireshark network packet / protocol analyzer was used for this aim as shown in Figure (5-a). The LAN network shown in this figure was used to monitor the server and the router as well as the service provider. Figure (5-b) depict the frame and the captured packets. Moreover, Figure (5- c) shows the series of packets sent and received.

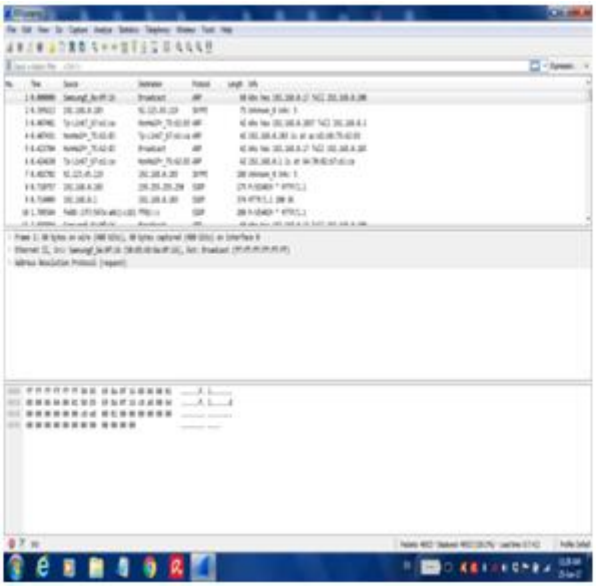
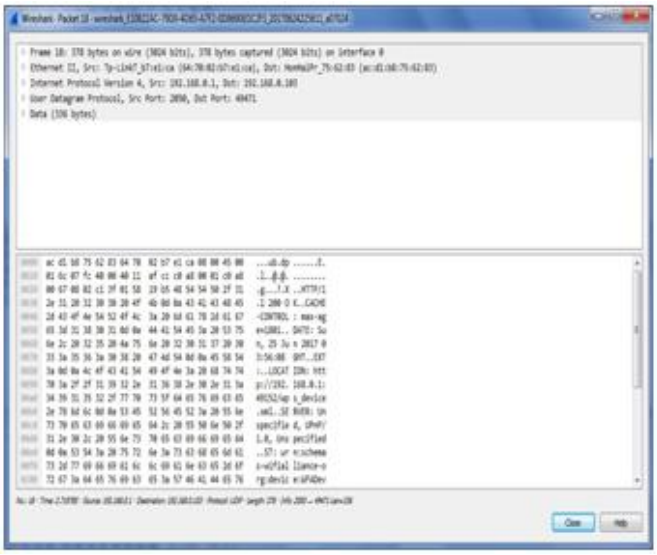


Figure [5-a]: Capturing wireless Network



Frame 18: 378 bytes on wire (3024 bits), 378 bytes captured (3024 bits) on interface 0
Ethernet II, Src: Tp-LinkT_b7:e1:ca (64:70:02:b7:e1:ca), Dst: HonHaiPr_75:62:83 (ac:d1:b8:75:62:83)
Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.103
User Datagram Protocol, Src Port: 2050, Dst Port: 49471
Data (336 bytes)

Figure [5-b]: Frame and Captured

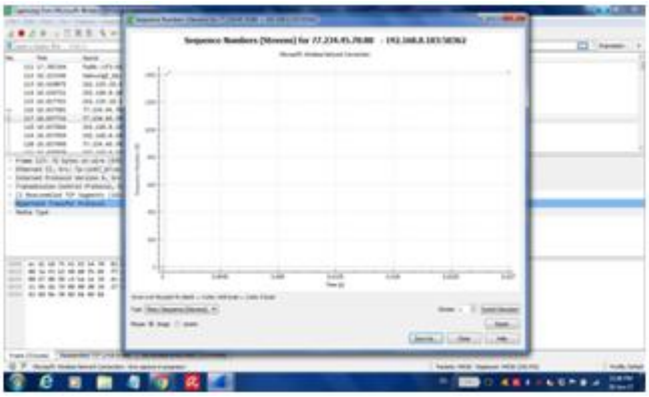


Figure [5- c]: Time Sequence Packets

The following Frame structure and Transmission Protocol was used as testing data project:

17. Fuzzification and Decision Making

Membership function for the captured packets of the LWSN mimic rules in section 12 to decision making according to risk minimizing aim such that:

$$\mu^{high}(x) = \begin{cases} 0 & x \leq 2.85 \\ (x-2.85)/_{2.5} & 2.85 < x \leq 4.5 \\ 1 & x > 4.5 \end{cases} \quad \ldots\ (6)$$

$$\mu^{average}(x) = \begin{cases} 0 & 0.5 < x \leq 1.5 \\ (2.85-x)/_{1.5} & 1.5 < x \leq 2.5 \\ 1 & x > 4.5 \end{cases} \quad \ldots\ (7)$$

$$\mu^{Low}(x) = \begin{cases} 0 & x \leq 0.5 \\ (0.5-x)/_{1.5} & 0.5 < x \leq 2.5 \\ 1 & x > 2.5 \end{cases} \quad \ldots\ (8)$$

Figure 6 depict risk surveillance with adapted fuzzy rules while Figure 7 represent results by surface.

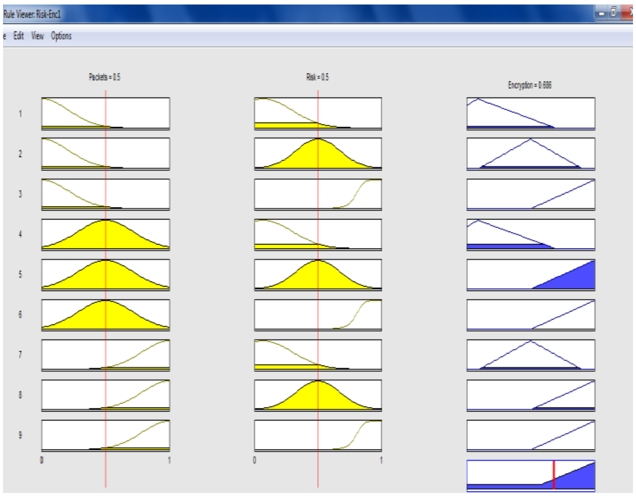
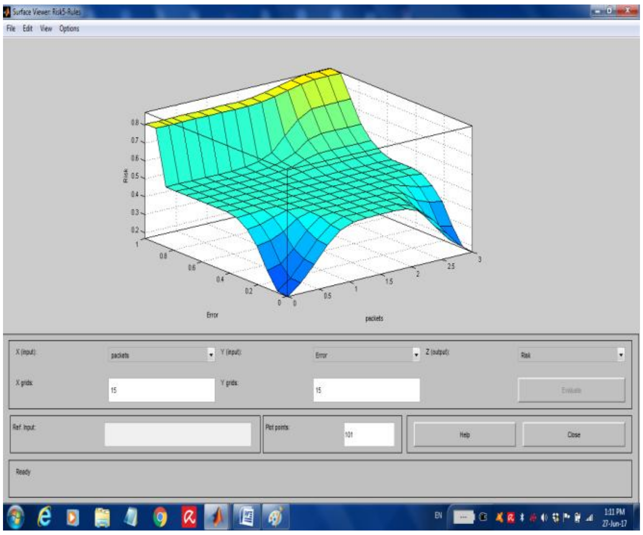


Figure 6: Risk Surveillance with Fuzzy Rules

Table 1: Frame Data

Frame 18	378 bytes on a wire (3024 bits)	378 bytes captured (3024) bits
Ethernet II	Src:TP-Link_TP7:e1:ca	Dst:HonHaipr_75:62:83
UDP	Src port :2050	Dst:192.168.0.103
Data	336 bytes	



X (input): packets
Y (input): Error
Z (output): Risk
X grids: 15
Y grids: 15
Ref. Input:
Plot points: 101
Ready

Figure 7: Surface Representation for Proposed Risk Surveillance

Table 2: Risk Compromising

Packets	Enc	Risk
Low	Neg	Low
High	Pos	Low
Low	Neg	Med
High	Pos	Med
Low	Neg	High
High	Pos	High
Low	Neg	Very Low
High	Neg	Very Low
Low	Neg	Very High
High	Pos	Very High

References

[1] Choi1, Robles, and Kim**,** Wireless Network Security: Vulnerabilities, Threats and Countermeasures, International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July 2008.

[2] Bhatia and Sumbaly**,** Framework for Wireless Network Security Using Quantum Cryptography, department of Computer Science in Dubai, UAE, 2013.

[3] Waliullah and Gan, Wireless Network Security: Vulnerabilities, A Literature Review, International Journal of Advanced Computer Science and Applications, Vol. 5, No. 1, 2014.

[4] Md Waliullah, Moniruzzaman and Rahman, An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network, International Journal of Future Generation Communication and Networking Vol. 8, No. 1 (2015),pp.9-18

[5] P. Kahai, S. Kahai, “Deployment Issues And Security Concerns With Wireless Local Area Networks: The Deployment Experience At A University” Journal of Applied Business Research, 2004, vol. 20, no. 4.

[6] Liu.Tao,, chen.Zheng,&Liu.Shengping, An Evaluation of Feature Selection for Text Clustering,Nankai University,2002.

[7] J. Lyne, “Hot Tipes for Securing Your Wi-Fi Network”, 2012.

[8] Shange and Hossen, Applying Fuzzy Logic to Risk Assessment and Decision-Making, Canadian Institute of Actuaries, Society of Actuaries, 2013.

[9] Sedghi and Kaghazgaran, Data Security via Public-Key Cryptography in Wireless Sensor Network, International Journal on Cybernetics & Informatics (IJCI) Vol.2, No.3, June2013.

[10] Malik, Kapoor, Naryan, and Singh, Rule Based Technique detecting Security attack for Wireless Sensor Network Using Fuzzy Logic , International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012.

[11] Shank, Kailan, and Hossen, Applying Fuzzy Logic to Risk Assessment and Decision-Making, 2013 Casualty Actuarial Society, Canadian Institute of Actuaries.

[12] Mooney, Raymond, Machine learning, Oxford handbook of computational linguistics, 2005.

Author Profile

Dr. Abdulkareem Merhej Radhiis Assist. Prof. and Doctorial Philosophy in Artificial Intelligence. Supervisor of many M.Sc. students in Information Engineering Colleges rather than Science Colleges. Lecturer in Al-Nahrain University. Director 0f Computer Center and AvinCina for E-Learning. Interested in Data Security, Soft Computing, Distributed Database, Engineering Analysis, Wireless Networks, Data Mining and Social Network Analysis.