International Research Journal of Management, IT & Social Sciences
Available online at https://sloap.org/journals/index.php/irjmis/
Vol. 6 No. 5, September 2019, pages: 108~117
ISSN: 2395-7492
https://doi.org/10.21744/irjmis.v6n5.714

New Technique for Protecting Transmitted Data Via WLAN

Marchella Macarulli [a]

Article history:

Received: 09 March 2019
Accepted: 31 May 2019
Published: 23 August 2019

Keywords:

information;
interceptions;
networking;
transmission;
wireless;

Abstract

The proposed work is a new technique for protecting the transmitted data via WLAN from eavesdropping and illegal interceptors. The main aim of this technique is to control the transmitted packets in order to minimize risks level which may be caused by probable attacks. Moreover, this technique assumes that the transmitted data in the training phase was used to train the system to be adaptable and immune against different attacks which may be caused within several circumstances. This proposed research covers all the possibilities using the framework of fuzzy theory for all risks levels and the size of every packet from low to high.

Author correspondence:
Marcel Macarulla,
GRIC, Department of Project and Construction Engineering, Universitat Politècnica de Catalunya, Spain.
Email address: marcel.macarulla@gmail.com

1. Introduction

Wireless networking presents many advantages productivity and economically that improves transmission speed of the huge data after the growth of demand to utilize information resources to support decision making. "However, wireless technology also creates new threats via alters the existing transmitted information (Sahu *et al.*, 2010)". Wireless networks transfer a huge amount of data, which is sensitive and vulnerable to interceptions than wired networks. "This would maximize the risk for users significantly and overcome these risks, wireless networks users choose to utilize various encryption methodologies". Encryption is the key to keep information secure online in a Wi-Fi network. However, "commonly utilized known encryption techniques have a big weakness and are susceptible by attackers via compromising confidentiality and risks (Soungalo *et al.*, 2012).

Due to the widespread use of wireless communication networks, the huge data passing via them, as well as their importance and confidentiality, are very important and a great goal to discover modern and new approaches protect data against various types of attacks and penetration. The proposed research is a new method to protect data from various unsafe and illegal threats which were discussed in later sections. This research aims to provide a new technology of constructing a smart and self-adaptive system based on the construction of different rules and aiming to encrypt data transmitted via wireless channels when they are aware of the level of risk. It is easiest and least expensive to protect data and achieve the maximum safety and it's designed to work in different circumstances, such as a noise

[a] Universitat Politècnica de Catalunya, Barcelona, Spain

that affect the accuracy of data sent, and invest the concepts of fuzzy theory to cover all possible probabilities of risk levels.

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. "WEP transfer data "as 64 bit or 128 bit but the actual transmission keys are 40 bits and 104 bits long where the other 24 bits is an Initialization Vector (IV) to send in the packet along with the data (Finneran, 2011)."

"The above vulnerabilities and threats arise are very important to make sure that the wireless network is secure whether for a home or an enterprise network." "The organization should implement continuous attack and vulnerability monitoring and perform a periodic technical security assessment to measure the overall security of the WLAN (Changping *et al.*, 2010)." "The use of strong encryption standards protects WLANs from the worst threats." The aim of this project satisfies this protection (Chandra & Lide, 2011).

This section presents various suggestions and different related techniques to protect transferred data. Jha *et al.*, (2014) suggest Quantum cryptography that "provides safety and security for network communication by performing cryptographic tasks using quantum mechanical effects." Fallah & Alnuweiri (2007), introduce public-key cryptography to "secure wireless network security which has been usually considered as nearly impossible."

Joseph *et al.*, (2012), conclude that key exchange protocols using optimized software implementations of public-key cryptography are viable on small wireless devices."

2. Materials and Methods

This proposed work is a new technique to protect the transmitted data via wireless networks from eavesdropping and illegal interceptors. The main aim of this technique is to manage and control the transmitted packets and construct a protection wall to minimize risks. Moreover, this technique assumes that the transmitted data was used as test data to test different attacks in several circumstances. This system detects the malicious activities and the illegal attacks that detect the active attacks which modify the transmitted data.

Unsupervised learning classifier was used to monitor the network and detect malicious intruders. The flow data have been collected and features are extracted and analyzed to examine the transmitted packets. Figure (1) depicts the architecture of the proposed system.

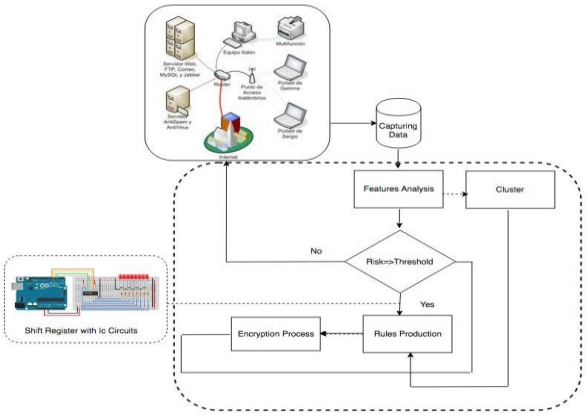

Figure 1. Architecture of the proposed system

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 of belonging to the same patterns. "Information gain (IG) 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, where (m) be the number of classes". The information gain of a term t is defined as*:*

$$\text{“IG(t)} = -\sum_{i=1}^{m} p(c)\, log\, P(c_i) + P(t)\sum_{i=1}^{m} p\left(\frac{c_i}{t}\right) log\, P\left(\frac{c_i}{t}\right) \dots\dots\dots\dots (1)\text{"}$$

Where t,c,m, and p are term, cluster, document, and probability respectively. To measure the association between each cluster, a term χ^2 used to define different clusters.

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

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

$$\text{“}(t) = -\sum_{i=1}^{N}\sum_{i=1}^{N}(S_{ij}\times \log S_{ij}) + (1-S_{ij})\times \log\,(S_{ij}(1-S_{ij}))\dots..(3)\text{"}$$

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

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

3. Results and Discussions

Entropy

To check the performance of the obtained classifier that detects the 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 contribute to risk analysis:

"Entropy (S) = $-p_+ \log_2 (p_+) - p_- \log_2 (p_-)$ - - (5)"
C

"Entropy (S) = $\sum_{I=1}$ - Pi log2 (Pi) --------- (6)"

Production of Fuzzy Renewable Rules

Production of fuzzy rules aims to construct a knowledge base of risk rules in two methods as follows:

1) Save 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."
2) Risk evaluation outcomes "flow into the risk decision-making process and the outcome of the decision can then are fed back into the system to refine the fuzzy sets, rules. Fuzzy logic models may be used with other risk models such as decision trees to model complicated risk issues ".

Performance measured in terms of recall and precision as follows:
Precision "measures the percent correct of instances extracted by the rule base [12]".

$$\text{"}Recall = \frac{No.\,of\ correctly\ predicted\ entities}{No.\,of\ entities\ that\ should\ been\ predicted}\dots(7)$$

$$Precision = \frac{No.\,of\ correctly\ predicted\ entities}{No.\,of\ all\ entities\ predicted}\dots.(8)\text{"}$$

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 the proposed system wall.

Minimizing risk

"The 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 (Mourad *et al.*, 2017; Musbah *et al.*, 2015)".

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: If (¬A ˜∧B) then G_3. G_2: **If** (G_3∨B) then G_4.*

The operands may assign numeric values.

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 (Garroppo *et al.*, 2016)". 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 the independent variable.

Algorithm

It was previously adopted algorithm to achieve two important features, the first one for data security transmitted over wireless networks and satisfying its reliability while the second property is the construction of a reliable security automated system. This research depicted in this paper approves a smart system via hardware implementation for security risk control depending on fuzzy concepts to cover all risk states with data code error exclusion. To have higher security for the transmitted data, which are formed as packets, we adopt the following algorithm:

a) Shift Register was used for this purpose of a length of 16 numbered packets.
b) The initial key is known only by the sender which represented by a Shift Register as a 16-bits long only.
c) There is a primary key of length 64 bits represented by (four Shift Registers) where each is 16 bits long.
d) Furthermore, relying on another key which is a message key of length 16 bits.
e) Every single bit of the message key integrates with Shift Register output for the primary key, according to the following sequence nonlinear the function:
$$O_n = Bk_{o_n} \oplus MK_{o_n}$$
f) All 16-bit per package integrates with outputs using XOR function.
g) Permutation and specific round function were used for the final output.
h) Finally, the output will be controlled using the following form: $O_{final} = O_n + \sim(P_k)$
Where P_k is packet bit number.
i) On the other hand, the recipient receives output data and opens the encrypted packets and reverse the cycle of the algorithm described in the previous points until the original package extracts the data.

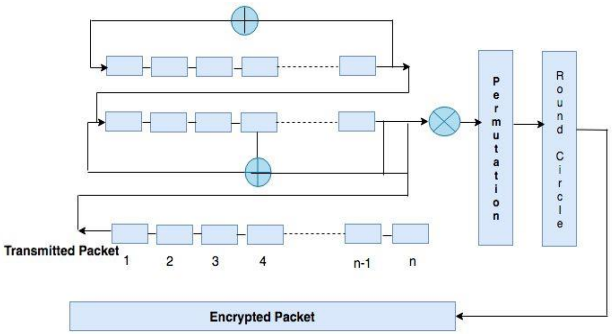

Figure 1. Block Diagram of the Encryption Process

Rule base

This paper adopts a fixed methodology in constructing a system of rules that are control data transmitted 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 rules which are the mathematical foundations of the proposed system: ("if risk then packets") are accepted, but the antecedent risk holds, then the consequent encryption cannot be activated.

a) ("if risk then packets") is accepted, but the consequent (packets) does not hold, then the negation of the antecedent encryption can be activated.
b) If ("risk and packets") are accepted but the consequent risk can be accepted then encryption cannot be activated.
c) If ("risk or packets") is accepted but the negation of antecedent (risk) holds then the encryption can be activated.
d) (" if risk then packets") is accepted, but the antecedent ("if risk then encryption") holds, then risk implies encryption can be activated.
e) If the risk is accepted and the antecedent packets hold, then the consequent risk and encryption cannot be activated. So we have to compromise between accepted risks and number of packet values which are gained from the practical tested proposed algorithm. The range of risk values is (0 to 4.5), while the range number of the accepted packets which is not affected by the type of attack technique is (100 to 100000).

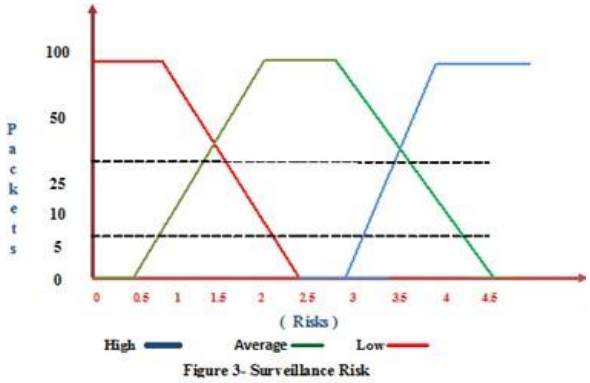

Figure 2. Surveillance Risk vice packets volume

Wireless software infrastructure

Figure (3) represents software infrastructure, where network link ETHERENT with TCP/UDP protocol to capture packets and analyze it.

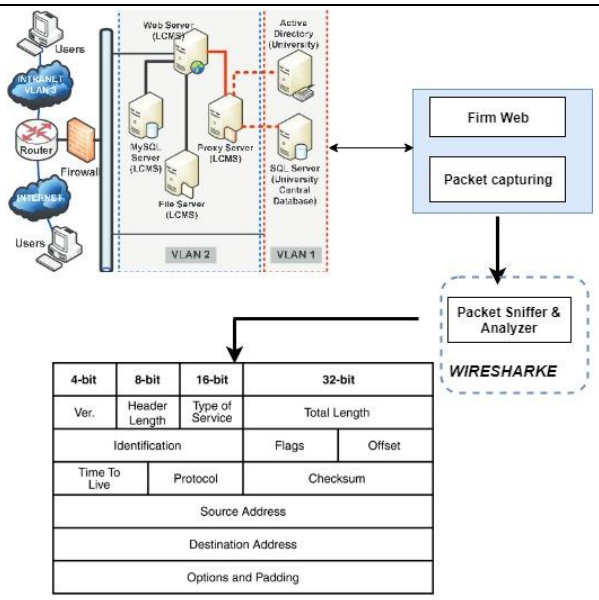

Figure 3. Wireless Software Infrastructure

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 objective. The LAN network was used to monitor the server and the router as well as the service provider. The proposed system depicts the frame and the captured packets and the time series of packets sent. Table [1] presents the frame structure and Transmission Protocol was used as testing data project, while Table [2] depicts cases of Risk Compromising.

Table 1
Structure of the 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	

Table 2
Risk compromising

Packets Size	*Encryption*	*Risk*
Low	*Negative*	*Low*
High	*Positive*	*Low*
Low	*Negative*	*Med*
High	*Positive*	*Med*
Low	*Negative*	*High*
High	*Positive*	*High*
Low	*Negative*	*Very Low*
High	*Negative*	*Very Low*
Low	*Negative*	*Very High*
High	*Positive*	*Very High*

Fuzzification and decision making

Membership function for the captured packets of the LWSN mimic rules that depicted in section VII to decision making according to risk minimizing aim such that membership functions between 0.5 and 4.5. So, the following (Low, Medium, and High) are the domains of membership function as follows:

Table 3
The captured packets of the LWSN mimic rules

Attack type	*Packets size*	*Encryption*	*Risk*
Masquerade	*Low*	*Negative*	*Low*
Rogue Point	*High*	*Positive*	*Low*
MITM	*Low*	*Negative*	*Med*
DOS	*High*	*Positive*	*Med*
Masquerade	*Low*	*Negative*	*High*
Rogue Point	*High*	*Positive*	*High*
MITM	*Low*	*Negative*	*Very Low*
DOS	*High*	*Negative*	*Very Low*
Masquerade	*Low*	*Negative*	*Very High*
Rogue Point	*High*	*Positive*	*Very High*

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

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

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

The estimated risk or loss of revenue is evaluated via two values, the size of the potential L loss, and the probability of loss. The risk or loss of revenue is:

$$R_i = L_{ip}(L_i) \ldots\ldots (9)$$
$$R_{total} = \sum_i L_{ip}(L_i) \ldots.. (10)$$

So, tables 4 depicts attack type and Probability of loss.

Table 4
Probability of loss

Attack type	Probability of Loss			Resources Damage
	Control	Product	Staff Time	
Reply	0.20	0.40	0.20	0.10
Spoofing	0.20	0.20	0.20	0.20
DOS	0.50	0.10	0.25	0.05
Control Message	0.15	0.05	0.10	0.50
Write to MTU	0.10	0.05	0.05	0.30

RTU Response	0.30	0.10	0.10	0.40
Write to RTU	0.30	0.20	0.20	0.20

While the values of a probability of loss for avoidance are: 0.10,0.20,0.10.0.20,0.50,0.10, and 0.10 respectively for all the types.

Decision making via WLAN attacks

All attacks to the transmitted data via WLAN are carried out by an interceptor or intruders in order to view or modify information for an organization. The general aim of these attacks is minimizing the confidentiality and availability of information and network.
Table [5] presents packets classification precision using equations 1,2,3, and 4 respectively.

Table 5
Sample packets classification precision

Term Index	*IG*	χ^2(t,c)	$S_{i,j}$	*Entropy*
0	2.31	*1,3*	*1.11*	*94.4*
1	3.41	*2,4*	*1.68*	*96.3*
2	3.34	*1,6*	*2.22*	*93.6*
3	6.67	*4,3*	*4.25*	*94.0*
4	4.22	*3,1*	*3.93*	*94.6*
5	1.35	*2,5*	*1.55*	*95.2*
6	3.51	*3,4*	*2.72*	*97.8*
7	2.22	*1,2*	*1.51*	*94.44*
8	4.51	*2,6*	*3.99*	*93.64*
9	2.90	*5,6*	*6.63*	*96.6*
10	5.55	*1,4*	*1.38*	*92.8*
11	4.18	*3,7*	*1.13*	*96.7*
12	5.92	*4,6*	*3.88*	*98.0*
13	8.90	*3,4*	*4.63*	*94.5*
14	3.67	*2,4*	*4.49*	*9.00*
15	1.98	*1,8*	*3.33*	*9.19*
16	2.68	*3,5*	*7.22*	*9.70*

In general, the attacker not only intercepts the information but also modify it and generate fake information on the network. The following are a list of active attacks in WLAN technology:

a) Unauthorized or Masquerade
b) Rogue Point
c) Man in the Middle (MITM)
d) Deny Service

Recall and precision depicted in equations 7 and 8 reflect after encryption a precision rate value 97% with very low minimum risk.

4. Conclusion

The proposed work is a new technique for protecting the transmitted data via WLAN from eavesdropping and illegal interceptors. The main aim of this technique is to control the transmitted packets in order to minimize risks level which may be caused due to probable attacks. Moreover, this technique assumes that the transmitted data in the training phase was used to train the system to be adaptable and immune against different attacks which may be caused within

several circumstances. This proposed research covers all the possibilities using the framework of fuzzy theory for all risks levels and the size of every packet from low to high.

Conflict of interest statement
The authors declared that they have no competing interest.

Statement of authorship
The authors have a responsibility for the conception and design of the study. The authors have approved the final article.

Acknowledgments
The authors would like to thank the editor of IRJMIS for their valuable time, support, and advice in completing the present research.

References

Chandra, P., & Lide, D. (2011). *Wi-Fi Telephony: Challenges and solutions for voice over WLANs*. Elsevier.

Changping, Z., Xingsong, D., Jia, Z., Lei, L. I., Xiaoyang, Z., Hongzhen, Y. U., & Zhang, S. (2010). Performance analysis of wireless local area networks (WLAN) in a coal-mine tunnel environment. *Mining Science and Technology (China)*, *20*(4), 629-634. https://doi.org/10.1016/S1674-5264(09)60257-X

Fallah, Y. P., & Alnuweiri, H. (2007). Hybrid polling and contention access scheduling in IEEE 802.11 e WLANs. *Journal of Parallel and Distributed Computing*, *67*(2), 242-256. https://doi.org/10.1016/j.jpdc.2006.07.003

Finneran, M. F. (2011). *Voice over WLANS: The complete guide*. Elsevier.

Garroppo, R. G., Nencioni, G., Scutellà, M. G., & Tavanti, L. (2016). Robust optimisation of green wireless LANs under rate uncertainty and user mobility. *Electronic Notes in Discrete Mathematics*, *52*, 221-228. https://doi.org/10.1016/j.endm.2016.03.029

Jha, S., & Ali, S. (2014, September). Mobile agent based architecture to prevent session hijacking attacks in IEEE 802.11 WLAN. In *2014 International Conference on Computer and Communication Technology (ICCCT)* (pp. 227-232). IEEE. https://doi.org/10.1109/ICCCT.2014.7001497

Joseph, W., Pareit, D., Vermeeren, G., Naudts, D., Verloock, L., Martens, L., & Moerman, I. (2013). Determination of the duty cycle of WLAN for realistic radio frequency electromagnetic field exposure assessment. *Progress in Biophysics and Molecular Biology*, *111*(1), 30-36. https://doi.org/10.1016/j.pbiomolbio.2012.10.002

Mourad, A., Muhammad, S., Al Kalaa, M. O., Refai, H. H., & Hoeher, P. A. (2017). On the performance of WLAN and Bluetooth for in-car infotainment systems. *Vehicular Communications*, *10*, 1-12. https://doi.org/10.1016/j.vehcom.2017.08.001

Musbah, E. M. M., Bilal, K. H., & Mustafa, N. (2015). Comparison of QoS performance over WLAN, VoIP4 and VoIP6. *International Research Journal of Management, IT and Social Sciences*, *2*(11), 29-37.

Sahu, B., Chakrabarti, S., & Maskara, S. L. (2010). An improved residual frequency offset estimation scheme for OFDM based WLAN systems. *Digital Signal Processing*, *20*(2), 454-461. https://doi.org/10.1016/j.dsp.2009.06.017

Soungalo, T., Renfa, L., Fanzi, Z., & Waita, H. N. (2012). Performance analysis of interworking between WLAN and 3G networks based on three approaches. *Procedia Engineering*, *29*, 1126-1132. https://doi.org/10.1016/j.proeng.2012.01.099