WEP and WPA Improvement

Prof. Awad H. Ali, Dr. Samani A. Talab, Mustafa ElGili

Department of Information Technology University of Neelain, Sudan, mustgili@hotmail.com

Abstract

This paper aims to describe a solution to improve wireless network security protocols WEP and WPA based on a modified RC4 algorithm for encryption, and based on IV with secret key for a session key exchange, and new mutual authentication mechanism.

Introduction

Wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. However, risks are inherent in any wireless technology. The loss of confidentiality and integrity and the threat of denial of service attacks are risks typically associated with wireless communications. WEP, WPA are designed to protect, but they still have weaknesses discussed in [2], [13], [12], [15], [20], [8], [6], [7],[8].

Related Work

Many solutions have been proposed for the remedy of the WEP and WPA encryption, key exchange and mutual authentication problems. Reference [10] proposes a scheme similar to WEP. The difference is that in EWEP it encrypts the concatenation of the message and IV with RC4. Encrypting IV aims to hide it from eavesdropping. This proposal has many weaknesses represented below:

1. Because IV[i+1] depends on IV[i], if some frames are lost, all frames coming from the same sender would not be decryptable.
2. It uses Diffe-Hellman [21] to agree IV, this is difficult because there is no clear share value.
3. Rekey is done using special messages. No protection mechanism for the messages contains the new key.
4. No new authentication mechanism described which means the authentication process is still weak.
5. It suffers from following attacks:
   - Disassociation and Deauthentication Attacks.
   - Shared Key Authentication Attacks.
   - FMS Attack.
   - Session Hijacking.
   - Reply Attack.

Reference [11] proposes new scheme which modifies the process of WEP Key generation on TKIP. Comparing with TKIP, the proposed protocol neither changes nor increases hardware cost. Moreover, it narrows down hardware computing quantities. Further, SEWTP reduces authentication frequency. It also provides security function as well as TKIP and does not affect the performance of throughput. But it has limitations represented as:

1. Over flooding, any client will send random number. New secret key has been generated before authentication process that leads to AP overload, because every client joining the AP domain will take a time to generate his secret key.
2. The clear IV still there.
3. Every 2^24 packet there will be random number from client to AP, this will lead to:
   - Over load traffic.
   - Overload in process time.
4. It suffers from the following attacks:
   - Disassociation and Deauthentication Attacks.
   - Shared Key Authentication Attacks.
   - FMS Attack.
   - Session Hijacking.
   - SYCH attack.

Proposed solution: WEP and WPA Improvement

We will propose a novel schema which essentially consists of three mechanisms:

a. Mutual Authentication between AP and Station.

b. Session Key Exchange mechanism.

c. Strong Encryption Protocol using modified RC4, and IV shadow.

a. Mutual Authentication Process and Session Key Exchange:

This is a solution for weak authentication in Wireless LAN which uses pre-shared key authentication, and also can be used in enterprise solution without any third party. The mutual authentication mechanism and Session Key Exchange mechanism consisting in the following steps:

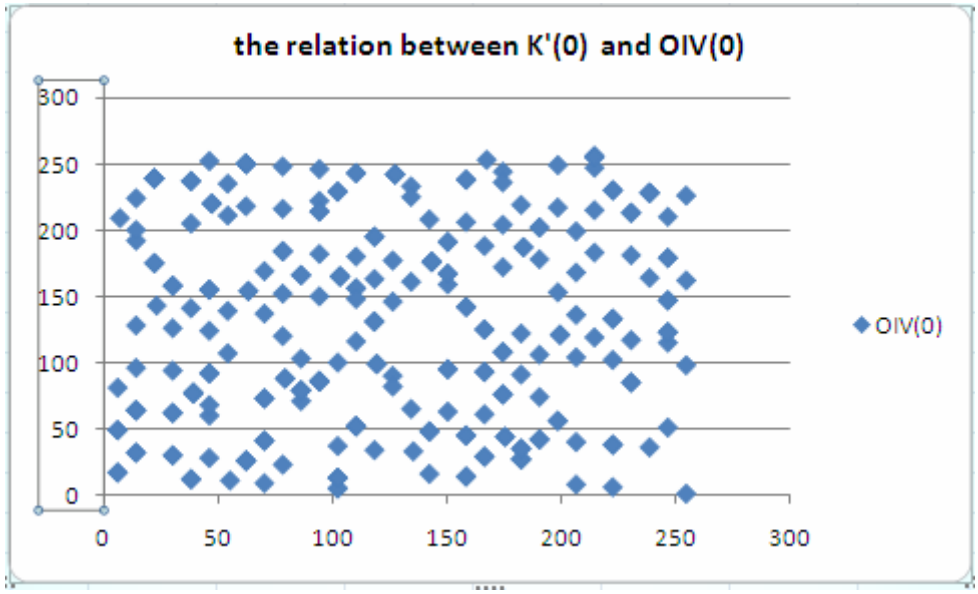
1. The first step stores the challenge value in the Station like secret key similar to Access point.
2. The second step: When the Station sends associate request to the Access point, the Access Point sends encrypted challenge with the secret key to Station.
3. The Station receives the Encrypted challenge and decrypts it using the secret key and Access point IV, and compares it with the challenge it has. If they are equal that means this Access point is trusted.
4. If this Access Point is trusted Calculate K',IV' using equations 1,2 respectively, and uses them with K(secret key), to encrypt the challenge again and sends it to the access point.
5. Update the Station challenge by adding IV' to old challenge.
6. The Access Point receives the Encrypted challenge and calculates the K', IV' and uses them with K(secret key), to decrypt challenge if it is equal to the challenge sent. This means the Station is trusted.
7. Update Access point challenge by adding IV' to old challenge.

b. Session Key Exchange mechanism:

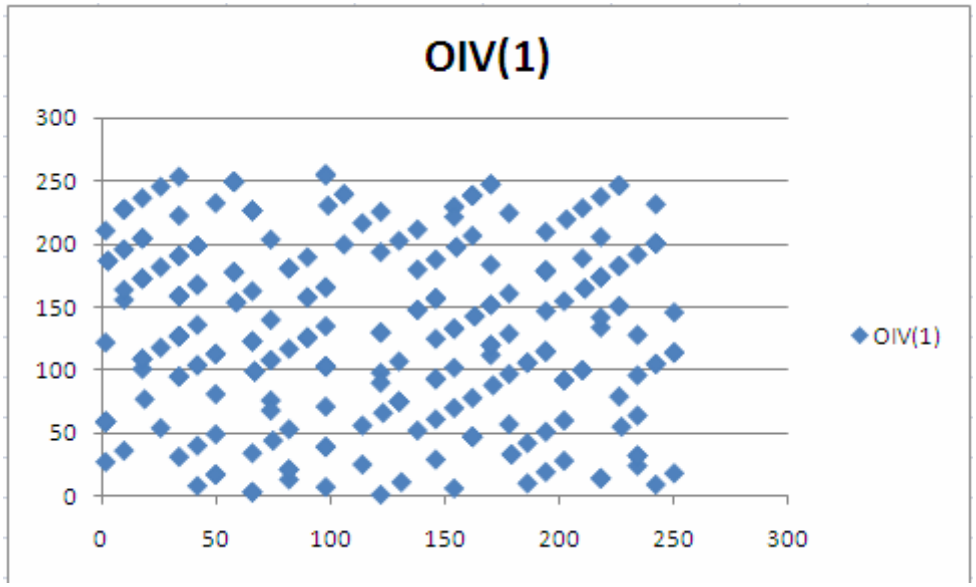
During Authentication process, we can calculate the session key, by using the equation below:

k'= $(IV_{old} + IV_{new})$+ $K^{(}$ +k[i+3] (1)

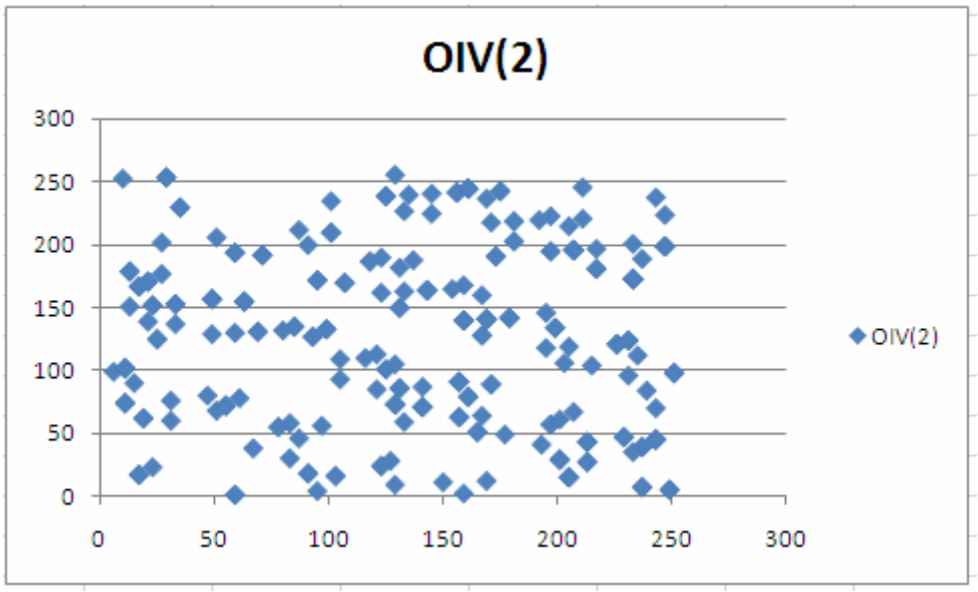
The result of using equation(1) to calculate K' shown in figures(1), (2), (3), they explain that there is no linear relation between old IV[i] and K'[i].



Fig(1) shows the relation between k'[0] and old IV[0]



Fig(2) shows the relation between k'[1] and old IV[1]



Fig(3) shows the relation between k'[2] and old IV[2]

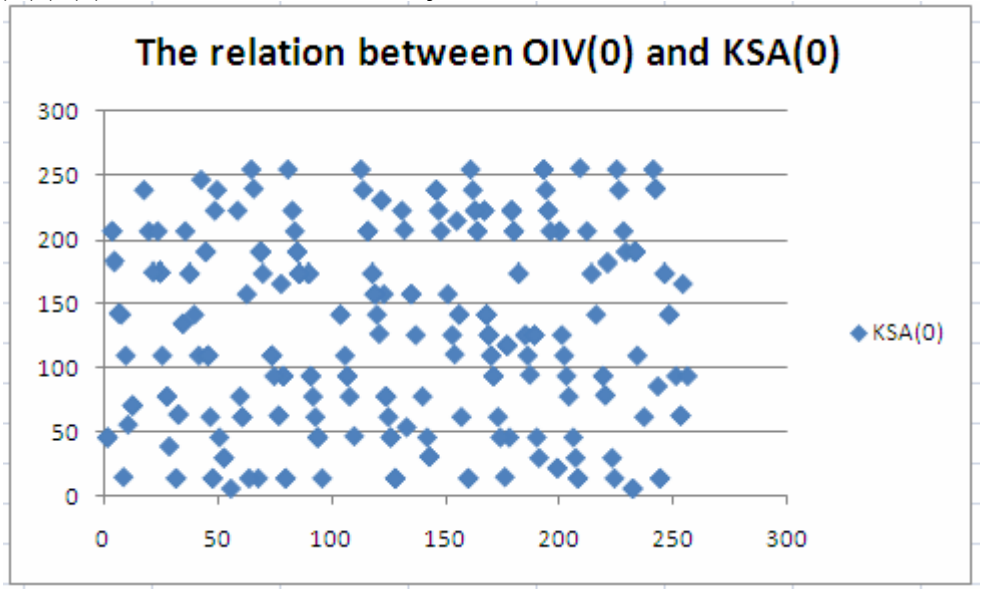
c. Strong Encryption using modified RC4:

We modified RC4 to be suitable for use with our approach, by using K' instead of feedback j as it is shown in algorithm below. To prevent first byte attack [9], and inverse attack:

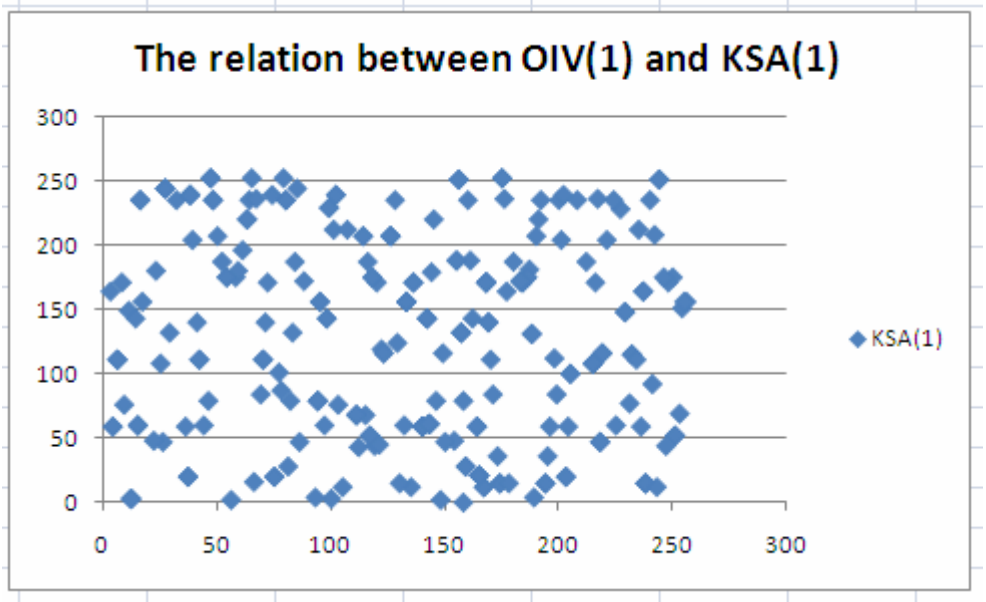
RC4 Modified key scheduling algorithm:

1: {initialization}
2: for *i* from 0 to *n* − 1 do
3: *S*[*i*] := *i*
4: end for
5: *j* := 0
6: {generate a random permutation}
7: for *i* from 0 to *n* − 1 do
8: j :=(K'[I mod e]+S[i]+ K[I mod l])mod n
9: swap S[i] and S[j]
10: end for

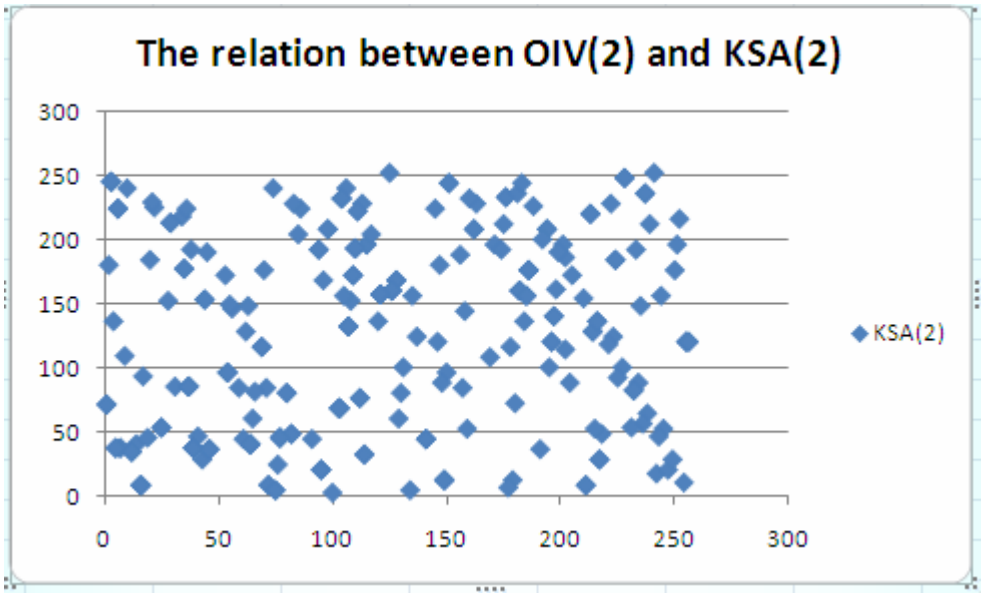
As a result of simulation test there is no linear relation between KSA[i] and old IV[i] as shown in figures (4),(5),(6). Which means the first byte attack cannot succeed.



Fig(4) shows the relation between old IV[0] and KSA[0]



Fig(5) shows the relation between old IV[1] and KSA[1]



Fig(6) shows the relation between old IV[2] and KSA[2]

1. An encryptor and Decryptor that share a RC4 secret key (K) agree session key or day key depending on the security level that they need. Using equation (1).

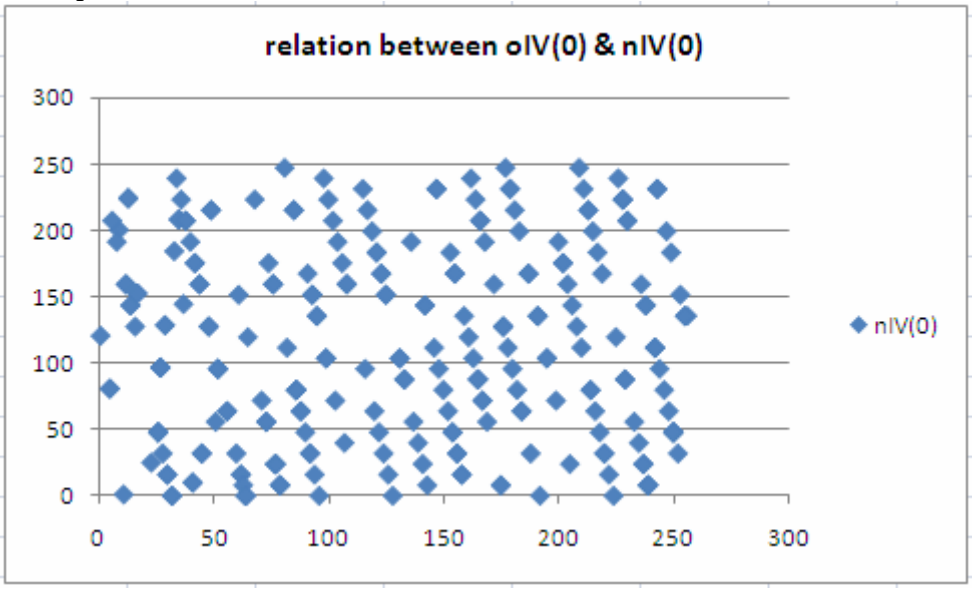
Where is K' represent session key or day key.

2. The secret key K uses to confuse IV to generate IV' which will combine with K to generate RC4 key seed as follows:

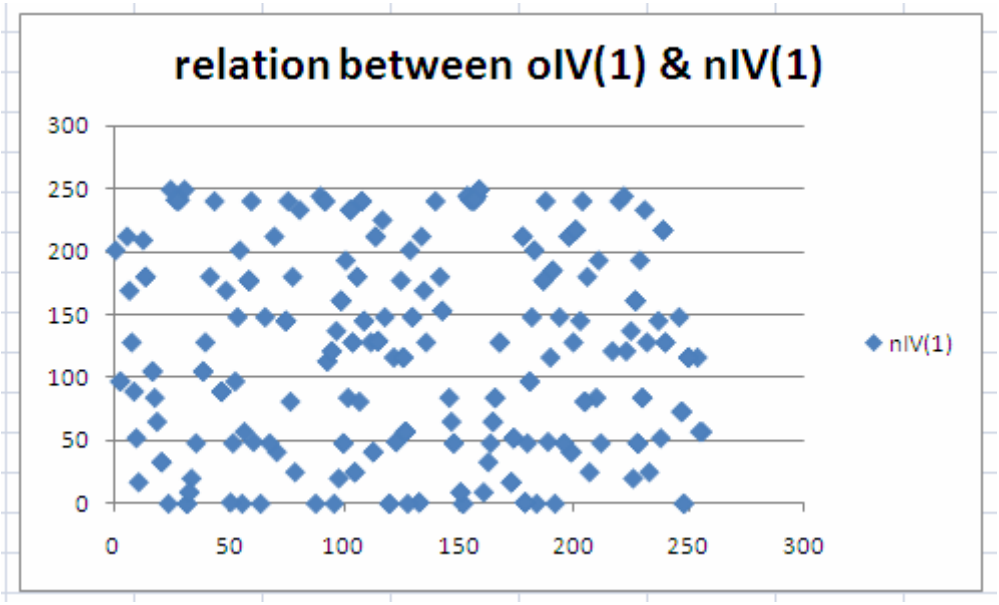
For i=o; IV length; {

$$IV' = ((IV * k + IV^{k[i \bmod 11]^i}) \bmod 256 \} \quad \textbf{(2)}$$

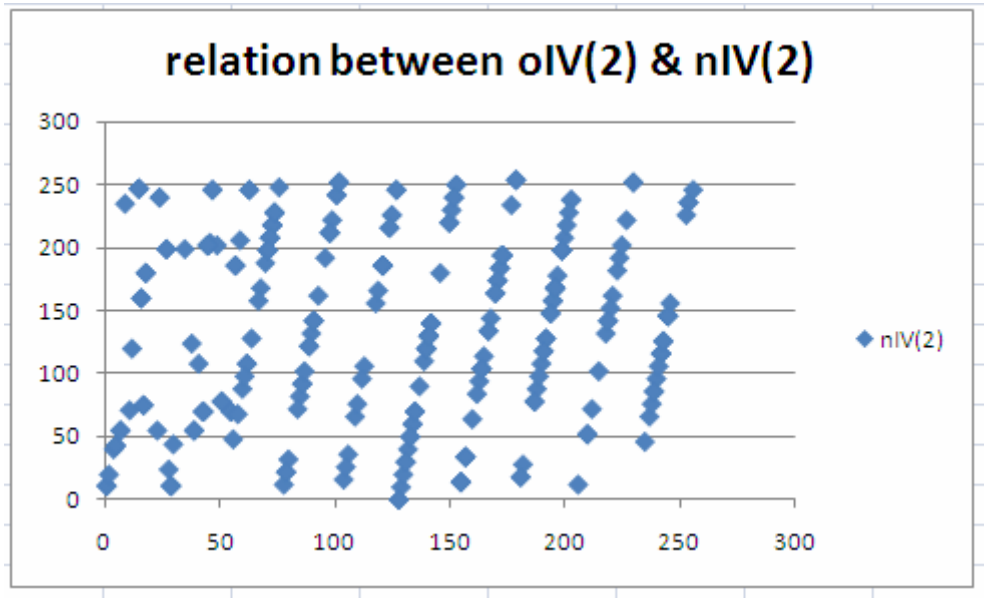
From the results of equation (2) there is no linear relation between new IV[i] and old IV[i] as shown in figures (7),(8),(9). This means that we can send the old IV as plaintext. The attacker can not use it to decrypt the ciphertext.



Fig(7) shows the relation between oIV[0] and nIV[0]



Fig(8) shows the relation between oIV[1] and nIV[1]



Fig(9) shows the relation between oIV[2] and nIV[2]

3. Combine the secret K and IV', with K' they will be the seed for RC4 algorithm.
4. Send cipher text and IV.

Comparison the IV value rollover:

For a device sending 10000 packets per-second

1. 24-bits, an IV will be reused after 16777216 packets, after 27,9 min.[WEP static secret Key]
2. 48-bit, an IV will be reused after 281474976710656 packets, after 892.6 years. [WPA static secret Key]
3. 24-bits, an IV will be reused after 16777216*39*13*16= 136096776192 packets, after 5.2 month.[Dynamic Session Key].

Comparison the Bandwidth overhead:

For a device sending 10000 packets per-second:

1. WEP overhead 44byte per-packet, means every second 4.4kbyte.
2. WPA overhead 56byte per-packet, means every second 5.6kbyte.
3. Our approach overhead 44byte per-packet means, 4.4kbyte.

References:

[1] Ron Rivest RSA Security Response to Weaknesses in key Scheduling Algorithm of RC4. (Feb 2002). www.rsasecurity.com/rsalabs/technotes/wep.html.
[2] WEP Fix using RC4 Fast Packet Keying. (Feb 2002). www.rsasecurity.com/rsalabs/technotes/wep-fix.html
[3] Vebjorn Moen & others . Weaknesses in Temporal Key Hash of WPA. (April 2004) www.nowires.org/Papers-PDF/WPA_Attack.pdf
[4] Adam Browning. The Limitation of WEP and The Advantages of WPA. (March2005). www.islab.oregonstate.edu/koc/ece478/05Report/Browing.pdf
[5] Erik Zenner. Why IV Setup for Stream Cipher is Difficult. (March 2007). www.erikzenner.name/docs/200_Dagstuhl_paper.pdf
[6] TakehiroTakahashi. WPA Passive Dictionary Attack Overview. www.personalwireless.org/tools/WPA-Cracker/ WPA_ Passive Dictionary_Attack_Overview.pdf
[7] Vebjørn Moen, Håvard Raddum, and Kjell J. Hole. Weaknesses in the Temporal Key Hash of WPA, https://bora.uib.no/bitstream/1956/1901/21/Paper4 Moen .pdf
[8] Drew Kalina (March 2005). WAP, WPA, and EAP islab.oregonstate.edu/koc/ece478/05Report/Kalina.doc
[9] Andreas Klein (February 27, 2007) Attacks on the RC4 stream cipher
[10] Hani Ragab Hassan, Yacine Challal. Enhanced WEP: An efficient solution to WEP threats.
[11] Jin-Cherng Lin, Yu-Hsin Kao. Secure Enhanced Wireless Transfer Protocol. Chen-Wei Yang Department of Computer Science and Engineering Tatung University. jclin@ttu.edu.tw, hebe@dlit.edu.tw, ychenwei@tcts.seed.net.tw
[12] ANKIT JAIN, SUMIT KARAN. WIRELESS LAN SECURITY
[13] Shefali Jariwala April, 2004. Enhancing Wireless Security with WPA
[14] Vishesh Kumar. High Speed Networks, Security in Wireless Networks
[15] Md Sohail Ahmad, Vivek Ramachandran. Cafe Latte with a Free Topping of Cracked WEP - Retrieving WEP Keys From Road Warriors
[16] Rajini Ananthoj and others. Network Security
[17] Allam Mousa and Ahmad Hamad(2006) Evaluation of the RC4 Algorithm for Data Encryption
[18] Jose Perez. A SURVEY OF WIRELESS NETWORK SECURITY PROTOCOLS. Texas A&M University – Corpus Christi
[19] Raj Jain(2007). Wireless LAN Security II: WEP Attacks, WPA and WPA2, Washington University in Saint Louis
[20] Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu, SECURITY IN WIRELESS LOCAL AREA NETWORKS. Department of Computer Science &Engine
[21] William Stallings,"Cryptography and Network Security", Third Edition(1999).

Article received: 2009-08-18