Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN

Vinay Bhatia
Department of ECE
Baddi University of Emerging Sciences and Technology, INDIA

Dushyant Gupta
Department of Electronic Science, Kurukshetra University, INDIA

H.P. Sinha
Department of ECE
M.M University
INDIA

ABSTRACT
Recent years have shown an unprecedented growth in the use of wireless LANs. However unlike the relative simplicity of wired Ethernet deployments, IEEE 802.11-based wireless LANs use radio-frequency (RF) data which is vulnerable to various attacks. This paper analyzes the IEEE 802.11b wireless LANs to determine variations in throughput so as to compare it for different standards. In addition the throughput is compared with a new hypothetical standard which is based on IEEE 802.11b. This paper also explores the vulnerability of these standards by simulating a popular attack on IEEE 802.11b wireless LAN. The simulations are carried in NS2 which are used to compare the total time utilized for various simulated standards. To have an enhanced insight of vulnerability of wireless LAN average time per symbol is calculated for various standards and has also been compared. Finally, we have implemented these results to derive dependency of vulnerability on key size length by obtaining a graphical and mathematical relation among them.

General Terms
Computer networks, wireless security, security algorithm.

Keywords
TKIP, WEP, WLAN, Wireless LAN.

1. INTRODUCTION
Today, wireless technology is a vital component that is being implemented in almost all sorts of business and personal communication purposes. During past few years, we have witnessed the deployment of astonishing number of wireless LAN networks. This enhanced popularity of wireless networks, such as wireless LANs, is on account of ease of installation of such networks, the low investment running cost, and the mobility in comparison with their wired counterparts [1]. However, with the widespread use of wireless networks, securing data from eavesdroppers has become a great challenge.

Various standards have been issued from time to time to address to the security problems associated with wireless LANs. Typically the IEEE 802.11 committee had developed an encryption mechanism known as Wired Equivalent Privacy (WEP) in the 802.11b wireless communications standard [2-6]; WEP is intended to provide security is equivalent to a similar wired network and is the part of IEEE 802.11wireless networking standard for securing the Wi-Fi networks, but suffers from several weaknesses [3-7].

1.1 Weaknesses in WEP
One of the key reasons of WEP's weakness is that the Initialization Vector (IV) used is very short and is reused very often [8-10]. If a hacker happens to capture two data packets with the same initialization vector, he can drudge the secret key S_k .This can be done by implementing XOR operation on the two packets which can be identified by cancellation of the key stream. Once two packets encrypted with same Initialization Vector (IV) are discovered, other methods of attacks can be applied to recover plain text (T_p). Key management is another weakness which is being suffered by IEEE 802.11 standard. WEP keys tend to be long lived and also most of the wireless networks use a single key, shared among all nodes of the network. Thus entire wireless network traffic, from all users, is encrypted with the same key that increases its vulnerability. One of the public attacks against WEP exploits a weakness in RC4, when certain values of Initialization Vector (IV) are realized [7].

1.2 Attacks on WEP
Since the network layers are common in wired and wireless networks, most of the attacks in the wired network will also work against wireless LANs. However, due to the characteristics of radio links, locating a hacker or an infected machine is always difficult in a wireless LAN. Thus it is more vulnerable to sniffing, brute force attack, worms and Trojans [10].

1.2.1 Dictionary Attack
A dictionary attack exploits the basic tendency of users to use weak passwords. In this attack, the wireless LAN is subjected to defeat by determining its secret key by repeatedly trying different passwords from a standard set, which in cryptography is known as the dictionary; hence the name Dictionary Attack [11-13]. Let us consider this challenge–response transaction between a sender S and receiver R which is commonly used in authentication protocols. In this transaction, both nodes can generate a random string. This string is transmitted to the other node so that it can encrypt the string with the key it has. The encrypted response is returned to the sender node and this is sufficient to guarantee that the peer does in fact posses the appropriate key. Let us consider a typical situation shown in Fig. 1. In this the sender S generates a random data packet (D_p) and sends it to receiver R after encrypting it using the secret key S_k. This forms a challenge for the receiver R. R decrypts, calculates D_p +1 and returns it back to S after encryption.

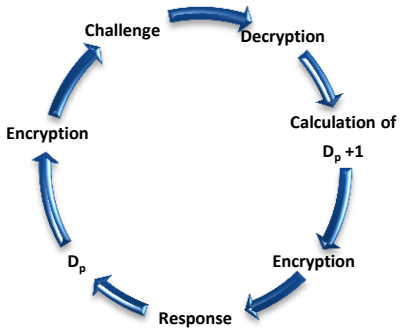

Fig 1: Challenge–Response transaction

However if secret key S_k is a weakly chosen password, and it belongs to a set of words in the dictionary D, then the

challenge – response transaction can be attacked. The intruder guesses a key $G_k \in D$ and tries to decrypt both messages D_p and $D_p + 1$ with the guessed key (G_k). Using this key the intruder obtains two values, P and Q respectively. If P = Q + 1, then the attacker has deduced the correct secret key $S_k = G_k$.

1.2.2 Brute force attack

In cryptography, a brute-force attack is a comprehensive key search that can, in theory, be used against any encrypted data. It involves systematically checking all possible keys until the correct key is found. In the worst case, complete search space may be exhausted during navigation. The key length used in the encryption determines the realistic feasibility of performing a brute-force attack. Brute-force attacks can be made less effectual by camouflaging intended sense of the data to be encoded, something that makes it more difficult for an attacker to recognize even when intruder has cracked the code [14, 15].

2. ALGORITHMS

The IEEE 802.11 wireless LAN uses WEP as an encryption mechanism WEP (Wired Equivalent Privacy) commonly known as IEEE 802.11b wireless communication standard [16, 17]. WEP is applied above the physical and data link layers of the OSI reference model. The basic intention to introduce WEP was to endow wireless LANs with a security equivalent to wired counterparts. To achieve these following three goals formed the part of WEP protocol:

• Concealment: The foremost goal of WEP is to provide security to a wireless LAN from an attack.

• Access control: The second goal of WEP aims in providing an access to the network only to valid users.

• Data reliability: Here data packet from the sender reaches in a form from which information can be readily extracted by the receiver.

Although WEP has provisions to achieve these goals as it uses CRC-32 for integrity check and uses RC4 cipher for encryption but the underlying algorithm was not properly implemented due to which WEP suffers various weaknesses.

2.1 Encryption Algorithm

The encryption algorithm that has been implemented in wireless LANs has a secret key S_k which is shared between the sender and the receiver and is used to encrypt the transmitted data. Once the sender has a message to be sent, it is considered to be as a plaintext. The plaintext feeds checksum algorithm using the CRC (Cyclic Redundancy Check) algorithm widely used in network protocols. Let us denote $N \longrightarrow £^{32}(T_p);$ is produced as a result that is further concatenated with the plaintext to produce N'. On the other hand, the Initialization Vector (IV) is concatenated with S_k and the resulting seed is used for generating a pseudo random sequence using PRNG A. This sequence is bitwise XORed with N'. The sequence so generated is called the Cipher Text and is finally transmitted along with Initialization Vector (IV) as the message packet. Here Initialization Vector (IV) is 24-bit long and the secret key is 40 bit long and has been named here as WEP-40.

WEP was vulnerable to many attacks. Hence a stopgap enhancement to WEP was also introduced in some of the early 802.11i drafts. This enhancement was implemented on some hardware which did not have the capabilities to handle other extended versions of IEEE 802.11 standards. This stopgap enhancement used 128-bit key values and is called WEP-128 in our paper. This paper presents a comparative analysis of these two standards in terms of their throughput and their strength against dictionary attacks. Further a hypothetical WEP with key values further extended to 256 bits called WEP-BGS, is simulated so as to compare its throughput with the other two standards already discussed. The algorithm of the WEP is depicted here, having following notations:-

Notations used

$£^{32}$ - Operation of CRC-32 algorithm

A - Operation of RC4 algorithm

$\oplus$ - XOR Operation

$\prod_C$ P - Concatenation

T_p - Plain Text

IV - Initialization Vector

S_k - Secret Key

C_t - Cipher Text

M_s - Message Signal

Algorithm of WEP

1. $N \longrightarrow £^{32}(T_p);$
2. $N' \longrightarrow \prod_C P(N, T_p);$
3. $M \longrightarrow \prod_C P(S_k, T_p);$
4. $X \longrightarrow A(M);$
5. $C_t \longrightarrow X \oplus N'$
6. $M_s \longrightarrow \prod_C P(C_t, IV);$

2.2 WEP Decryption Algorithm

The Decryption in wireless LANs is done using the algorithm depicted by flowchart shown in Fig. 2. In this algorithm the secret key S_k and Initialization Vector (IV) are concatenated to formulate a key, which is converted into a key sequence using RC4. The key sequence is XORed with the cipher text which results in plaintext. Now the ICV and plaintext are separated and the plaintext goes to Integrity Algorithm, constructing a new ICV called (ICV'). ICV and ICV' are compared to arrive at the decision of whether or not to accept the data packet as an information.

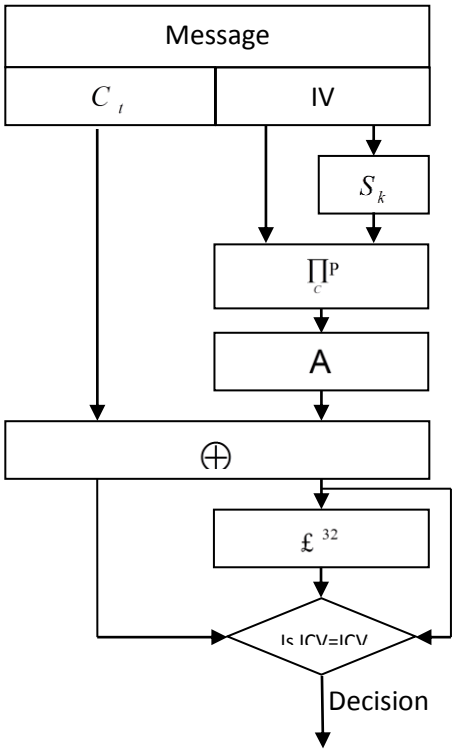

Fig 2: Decryption algorithm of WEP

3. SIMULATIONS AND RESULTS

3.1 Simulation Set-up

Modeling a wireless LAN with WEP is another important aspect of this work. For this, we have used NS2 to develop the simulation script when we first simulated the wireless LAN consisting of 50 nodes. In the first part of our simulation, we have obtained the variation of throughput for a standard WEP called WEP-40, WEP with increased key size called WEP-104 and finally for a hypothetical WEP called WEP-BGS with total key length of 256 bits. The second part of this section deals with vulnerability analysis of WEP with different key sizes. For this we have simulated a dictionary attack on WEP-40, WEP-104 and WEP-BGS. Further, the average time taken to recover a key has also been compared.

3.2 Performance Evaluation by Throughput Analysis

In this part of the section we present the Xgraphs of throughput variations with simulation time. Fig. 3 shows the variation of throughput for WEP-40 while Fig. 4 shows the throughput variation of WEP with increased key length i.e WEP-104. The variation of throughput in similar scenario for a hypothetical WEP called WEP-BGS are shown in Fig. 5 so as to understand the effect of increased key size on the throughput. Finally we compare the throughput of various algorithms in Fig. 6 by obtaining a combined Xgraph for all WEPs discussed. As observed from the graphs that after the initialization of data transfer the variation in throughput is more or less flat.

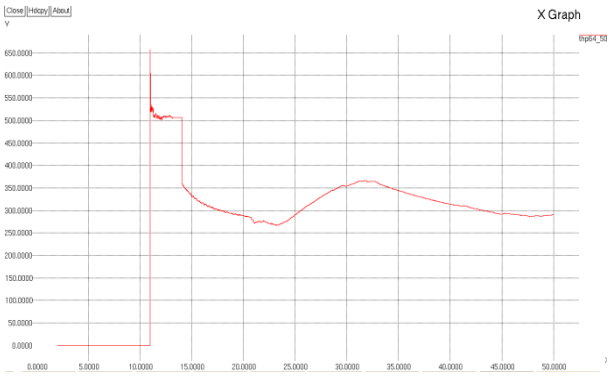

Fig 3: Throughput of a wireless LAN with WEP-40

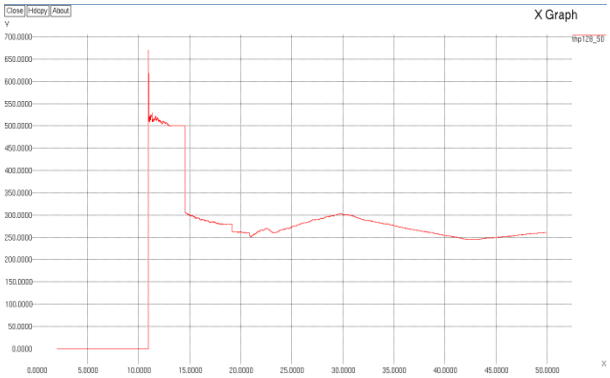

Fig 4: Throughput of a wireless LAN with WEP-104

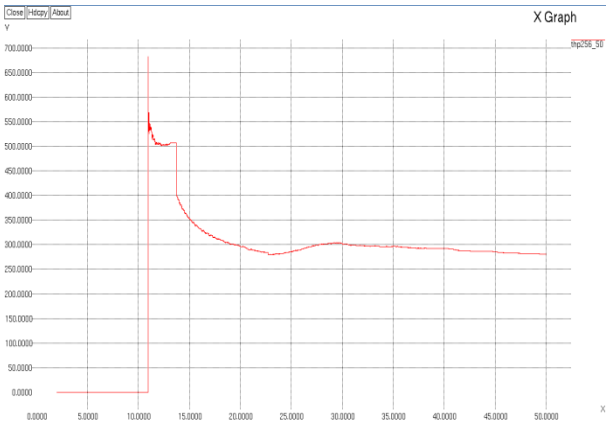

Fig 5: Throughput of a wireless LAN with WEP-BGS

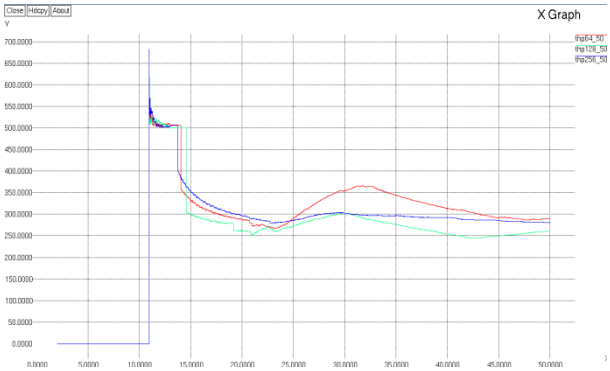

Fig 6: Comparison of Throughput variation of a wireless LAN with WEP of different key size

3.2.1 Comparison of average throughput

From the above graphs average throughput (kbps) is found for 50 nodes used in simulation environment using total simulation time of 50 seconds. The results are plotted in Fig. 7. As seen from Fig. 7 the maximum variation in average throughput limits up to 6 %.

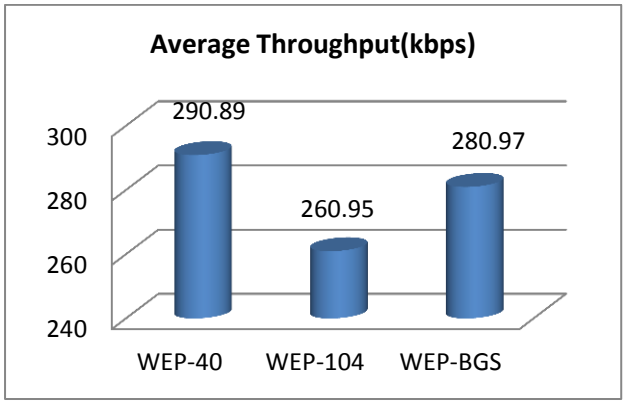

Fig 7: Average throughput for various algorithms

3.3 Performance Evaluation by Vulnerability Analysis

In this section we present the vulnerability analysis of the IEEE 802.11 wireless LAN. For this we have simulated dictionary attack, the most popular attack as it exploits the tendency of a user to use weak passwords. The attack is implemented on simulated IEEE 802.11b wireless LAN with different key sizes. Each simulated wireless LAN is subjected to the attack for 10 times to obtain total time to extract the key. Finally the averaged total time τ_t to extract the key is found from these ten repeated observations.

3.3.1 Dictionary attack on WEP-40

The total time to extract the secret key S_k used in WEP-40 when subjected to dictionary attack and the average time to extract each symbol per the key are provided in table 1 using following parameters.

Number of nodes used in simulation environment: 50

Number of time simulation is carried out: 10

Total simulation time: 50 seconds

Table 1. Total time and average time per symbol to obtain key in WEP-40

Observation Number	WEP-40 Total Time	WEP-40 Average Time per symbol
1	112	1.75
2	149	2.328125
3	129	2.015625
4	89	1.390625
5	151	2.359375
6	145	2.265625
7	178	2.78125
8	169	2.640625
9	127	1.984375
10	119	1.859375

Total time (averaged) τ_t: 136.8

Average time per symbol τ_s: 1.96875

Standard deviation of total time (averaged) σ_t: 26.927

Standard deviation of total time per symbol σ_s: 0.421

3.3.2 Dictionary attack on WEP-104

The total time to extract the secret key S_k used in WEP-104 when subjected to dictionary attack and the average time to extract each symbol per the key are provided in table 2 using following parameters.

Number of nodes used in simulation environment: 50

Number of time simulation is carried out: 10

Total simulation time: 50 seconds.

Table 2. Total time and average time per symbol to obtain key in WEP-104

Observation Number	WEP-104 Total Time	WEP-104 Average Time per symbol
1	375	2.9296875
2	301	2.3515625
3	280	2.1875
4	227	1.7734375
5	304	2.375
6	197	1.5390625
7	158	1.234375
8	241	1.8828125
9	255	1.9921875
10	269	2.1015625

Total time (averaged) τ_t: 260.7

Average time per symbol τ_s: 2.037

Standard deviation of total time (averaged) σ_t: 60.705

Standard deviation of total time per symbol σ_s: 0.474

3.3.3 Dictionary attack on WEP-BGS

The total time to extract the secret key S_k used in WEP-BGS when subjected to dictionary attack and the average time to extract each symbol per the key are provided in table 3 using following parameters.

Number of nodes used in simulation environment: 50

Number of time simulation is carried out: 10

Total simulation time: 50 seconds

Table 3. Total time and average time per symbol to obtain key in WEP-BGS

Observation Number	WEP-BGS Total Time	WEP-BGS Average Time per symbol
1	375	2.9296875
2	301	2.3515625
3	280	2.1875
4	227	1.7734375
5	304	2.375
6	197	1.5390625
7	158	1.234375
8	241	1.8828125
9	255	1.9921875
10	269	2.1015625

Total time (averaged) τ_t: 538.2

Average time per symbol τ_s: 2.102

Standard deviation of total time (averaged) σ_t: 56.444

Standard deviation of total time per symbol σ_s: 0.220

Fig. 8 shows the comparison of average time to extract the secret key, τ_t by a dictionary attack on a wireless LAN of different key size. The comparison depicts an improvement in strength against the attack with increase in key size.

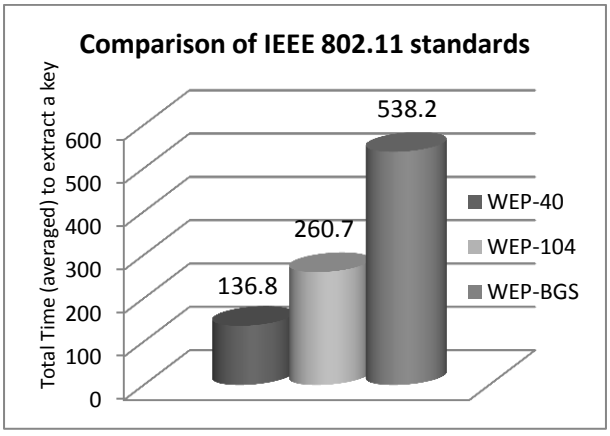

Fig 8: Comparison of Total Time (averaged) to extract the secret key for various IEEE 802.11 standards

Fig.9 shows the variation of average time per symbol for wireless LAN provided with security algorithm WEP of different key sizes. Finally the relation is found from the variation between average time taken per symbol to hack a key using dictionary attack on the most commonly used wireless LAN security standard WEP.

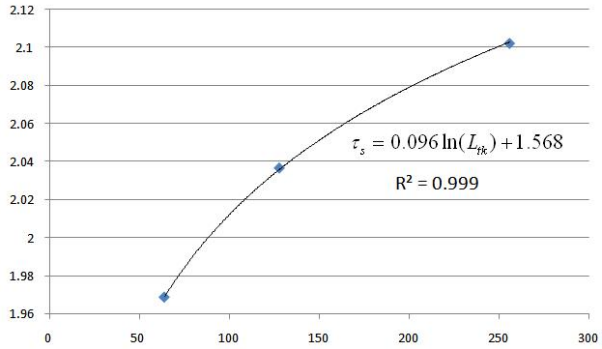

Fig 9: Average time per symbol vs key-size

From the above relation it is found that average time taken per symbol to hack key, τ_s is a function of length of total key L_{tk} and found to depend according to the following relation

$$\tau_s = 0.096\ln(L_{tk}) + 1.568$$

This shows the logarithmic improvement in time per symbol with increase in the length of total key.

4. CONCLUSION

In this paper we have presented analysis of a wireless LAN security with the commonly used security algorithm used by users and its vulnerability to the most popular attack with the attacker. There are two key parameters which form part of the analysis namely throughput and vulnerability. We have found that an increase in the key length does not affect the throughput of wireless LAN significantly, while some minor variations have also been observed. However, a noteworthy improvement in vulnerability is noted. We have found that total time to explore a key increase significantly with increase in key length. Finally we conclude that there is a logarithmic improvement in time to explore the key per symbol.

5. REFERENCES

[1] Kapp, S. 2002. 802.11: leaving the wire behind. IEEE Journal on Internet Computing, Volume: 6, Issue: 1, Page(s): 82 – 85.

[2] Wool, A. 2004. A note on the fragility of the "Michael" message integrity code. IEEE Transactions on Wireless Communications, Volume: 3, Issue: 5, Page(s): 1459 - 1462.

[3] Guelzim, T.; Obaidat, M.S. 2009. A new counter disassociation mechanism (CDM) for 802.11b/g wireless local area networks. IEEE/ACS International Conference on Computer Systems and Applications, Page(s): 251 – 259.

[4] Arbaugh, W.A.; Shankar, N.; Wan, Y.C.J.; Kan Zhang. 2002. Your 80211 wireless network has no clothes. IEEE Journal on Wireless Communications, Volume: 9, Issue: 6, Page(s): 44 – 51.

[5] Williams, J. 2001. The IEEE 802.11b security problem. IEEE Journal IT Professional, Volume: 3, Issue: 6, Page(s): 96, 91 – 95.

[6] Pahlavan, K.; Levesque, A.H.; 1994. Wireless data communications. Proceedings of the IEEE. Volume: 82, Issue: 9, Page(s): 1398 – 1430.

[7] Fluhrer, S.R., Mantin, I. & Shamir.A. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography, Page(s):1–24.

[8] Jagetia, M.; Kocak, T. 2004. A novel scrambling algorithm for a robust WEP implementation. IEEE 59th Vehicular Technology Conference Volume: 5, Page(s): 2487 – 2491.

[9] Songhe Zhao; Shoniregun, C.A. 2007. Critical Review of Unsecured WEP. IEEE Congress on Services, Page(s): 368 – 374.

[10] Steven Furnell and Bogdan Ghita. 2006. Usability pitfalls in Wireless LAN security Elsevier Journal Network Security, Issue 3, Pages 4-8.

[11] Delaune, S.; Jacquemard, F. 2004. A theory of dictionary attacks and its complexity. IEEE 17th Computer Security Foundations Conference, Page(s): 2 – 15

[12] Vykopal, J.; Plesnik, T.; Minarik, P. 2009. Network-Based Dictionary Attack Detection. IEEE International Conference on Future Networks, Page(s): 23 – 27.

[13] Petroni, N.L., Jr.; Arbaugh, W.A. 2003.The dangers of mitigating security design flaws: a wireless case study. IEEE Journal on Security & Privacy, Volume: 1 , Issue: 1, Page(s): 28 – 36.

[14] Couture, N.; Kent, K.B. 2004. The effectiveness of brute force attacks on RC4. Second Annual IEEE Conference on Communication Networks and Services Research, Page(s): 333 – 336.

[15] Seongyong Ahn; Hyejong Hong; Hyunjin Kim; Jin-Ho Ahn; Dongmyong Baek; Sungho Kang. 2009. A hardware-efficent multi-character string matching architecture using brute-force algorithm. International SoC Design Conference (ISOCC), Page(s): 464 – 467.

[16] Hwangnam Kim, Hou, J.C. 2004. Improving protocol capacity for UDP/TCP traffic with model-based frame scheduling in IEEE 802.11-operated WLANs. IEEE Journal on Selected Areas in Communications, Volume: 22 , Issue: 10, Page(s): 1987 – 2003.

[17] Bononi, L.; Conti, M.; Gregori, E. 2004.Runtime optimization of IEEE 802.11 wireless LANs performance. IEEE Transactions on Parallel and Distributed Systems, Volume: 15, Issue: 1, Page(s): 66 – 80.