Volume : 1, Issue : 1
January - June 2011

ISSN : 2229 - 3515

international journal of ADVANCES IN SOFT COMPUTING TECHNOLOGY

Editor-in-Chief
Dr.Vaka Murali Mohan

Published by
BHAVANA RESEARCH CENTER

Secured Quality of Service in Wireless Network

Prabhakara Rao, S[1]*., Nagabhooshanam, E[2] and Govardhan, A[3]
1.Head, Dept. of ECE, RRSCET. Muthangi (V) Patancheru(M),Medak (Dt), A.P, INDIA
2.Professor & Head, Dept. of ECE, M G I T, CB Post, Gandipet, Hyderabad, A.P, INDIA
3.Principal, JNTUJ College Of Engineering, Kodimyal(M), Karimnagar(Dt), A.P, INDIA

Key Words:
Wireless Networks 802.11, Block Cipher, Wireless Security, WEP, WPA, Throughput, Network Resource, Security Attacks, Cryptography.

Abstract: *Wireless network security based on encryption is widely prevalent at this time. However, encryption techniques do not take into account wireless network characteristics such as random bit errors due to noise and burst errors due to fading. We note that the avalanche effect that makes a block cipher secure also causes them to be sensitive to bit errors. This results in a fundamental trade-off between security and throughput in encryption based wireless security. The problem of bandwidth in Wireless networks based on a better security is been evaluated along with the evaluation of the impact of security mechanisms of WEP and WPA on the performance of networks 802.11g, considering which points are responsible for the decision on a specific kind of security to be used pondering factors such as the kind of network, since it could be in a home, company or both, logistics structure and network*

1. Introduction:

Wireless networks 802.11, became very attractive for both, domestic and corporative environment in the last few years. The reason for such diffusion is due to commercial availabilities, mobility, easiness of installation and flexibility, among others. Using air as a means of transmission turns wireless network into an insecure environment, an open door for malicious actions. In order to solve this problem, several mechanisms and security systems are being developed, and whenever well applied, they turn wireless networks secure and trustworthy. However, each mechanism has a performance price [1-2]. Wireless communication medium is open to intruders. In a wireless network, an eavesdropper can intercept a communication by listening to the transmitted signal. Hence, encrypting the transmitted packets helps to achieve confidentiality. Traditionally, the design of encryption algorithms and their parameters has used only security against an adversary attack as the main criterion.

**** Prof. S. Prabhakara Rao***
Head, Dept. of ECE
RRS College of Engineering and Technology
Muthangi (V), Patancheru (M),
Medak (Dt) 502 300, AP, INDIA
Ph. No.: 91-9490065307
E-mail: saggurthi_p@yahoo.co.in

To achieve this goal, the encrypted data or the cipher is made to satisfy several properties including the avalanche effect [3]. The avalanche criterion requires that a single bit change to the plain text or the key must result in significant and random-looking changes to the cipher text. Typically, an average of one half of the decrypted bits should change whenever a single input bit to the decryption device is complemented. This guarantees that there will not be any noticeable resemblance between two cipher texts obtained by applying two neighboring keys for encrypting the same plain text. Otherwise, there would be considerable reduction of the keyspace search by the cryptanalyst.

Since the securities structures are based on structural levels, the local networks are defined by residential and companies networks and are divided into mobile (notebooks) and fixed networks. The real purpose to define the networks in fixed and mobile will depend on the master problem of the security system, which has introduced that most attacks in companies come from inside the company. Therefore, wireless networks allow external users to become internals to the company, as well as it allows internals to create problems with equipment that go through different networks. The protocols of the Wi-Fi network include the specifications 802.11a, 802.11b, 802.1lg among others. For the standard IEEE (Institute of Electrical and Electronics Engineers) 802.11, WEP and WPA are seen as a service to the logical layer, supplied by the MAC sub-layer. The real execution of the service WEP and WPA is transparent to LLC and the other layers above the MAC sub-layer [4]. The PHY layer defines the characteristics and the transmission methods for the data reception. For the tests in

this article, equipments 802.1lg were used. They operate in the frequency of 2.4 GHz, with modulation OFDM and with theoretical rates up to 54Mbps.

2. Different modes in ciphers:

There are five basic modes of operation for a block cipher.

The Electronic CodeBook (ECB) mode,
Cipher Block Chaining (CBC) mode,
Cipher FeedBack (CFB) mode,
Output FeedBack (OFB) mode, and
CounTeR (CTR) mode.

Block Cipher Modes

Block ciphers operates on blocks of plain-text and cipher-text. The block size is usually 64 bits. Operating on blocks of 64 bits (8 bytes) is not always useful, and may be vulnerable to simple cryptanalysis attacks. E.g. the same plain-text always produces the same cipher-text, and is especially vulnerable to replay attacks. Several block cipher "modes of operation'' are in use today. The most common ones are described below.

Electronic codebook mode:

The simplest block cipher mode of operation is the electronic codebook mode (ECB). One block of plain text always produces the same block of cipher text. If crypt-analysts learn that the block "8d226acd" encrypts to the cipher-text block "1c7ed351", they whenever it appears in a message This vulnerability is greatest at the beginning and end of messages, where well-defined headers and footers contain information about the sender, receiver, date, etc.

Cipher block chaining

Cipher Block Chaining (CBC) uses feedback to feed the result of encryption back into the encryption of the next block. The plain-text is XOR'ed with the previous cipher-text block before it is encrypted. The encryption of each block depends on all the previous blocks. This requires that the decryption side processes all encrypted blocks sequentially. This mode requires a random initialization vector which is XOR'ed with the first data block before it is encrypted. The initialization vector does not have to be kept secret. The initialization vector should be a random number (or a serial number), to ensure that each message is encrypted uniquely. An error in an encrypted block (caused by e.g. a transmission failure) causes the block with the error to be completely garbled. The subsequent block will have bit errors at the same positions as the original erroneous block. The blocks following the second block will not be affected by the error. Hence, CBC is self-recovering. While CBC recovers quickly from bit errors, it does not recover at all from synchronization errors. If a bit is added or lost from the cipher-text stream, then all subsequent blocks are garbled. A system that uses CBC must therefore ensure that the block structure remains intact. Like the ECB mode, CBC also requires a complete block on its input before encryption can take place.

Cipher feedback (CFB)

The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher. Operation is very similar; in particular, CFB decryption is almost identical to CBC decryption performed in reverse. CFB shares two advantages over CBC mode with the stream cipher modes OFB and CTR: the block cipher is only ever used in the encrypting direction, and the message does not need to be padded to a multiple of the cipher block size.

Figure 1. 8 bit Cipher Feedback Mode

The initialization vector used in CFB mode has the same properties as the initialization vector used in CBC mode. It does not have to keep the secret, but should be different for every message transmitted with the same key.

Bit errors in the incoming cipher block (bytes in this context) will cause bit error at the same bit positions in the first plain text block. This cipher block will then be fed to the shift register and cause bit errors in the plain text for as long as the erroneous bits stay in the shift register. Hence, for 8-bit CFB the following 8 bytes will be garbled. After that, the system recovers, and all following bytes is decrypted correctly.

Output FeedBack (OFB) mode:

In OFB encryption, the IV is transformed by the forward cipher function to produce the first output block. The first output block is exclusive-ORed with the first plaintext block to produce the first ciphertext block. The first output block is then transformed by the forward cipher function to produce the second output block. The second output block is exclusive-ORed with the second plaintext block to produce the second ciphertext block,

and the second output block is transformed by the forward cipher function to produce the third output block. Thus, the successive output blocks are produced from enciphering the previous output blocks, and the output blocks are exclusive-ORed with the corresponding plaintext blocks to produce the ciphertext blocks.

CounTeR (CTR) mode:

The Counter (CTR) mode is a confidentiality mode that features the application of the forward cipher to a set of input blocks, called counters, to produce a sequence of output blocks that are exclusive-ORed with the plaintext to produce the ciphertext, and vice versa. The sequence of counters must have the property that each block in the sequence is different from every other block. This condition is not restricted to a single message: across all of the messages that are encrypted under the given key, all of the counters must be distinct. In this recommendation, the counters for a given message are denoted T1, T2, …. Methods for generating counters are discussed in Appendix B. Given a sequence of counters, T1, T2, …, Tn, the CTR mode is defined as follows:

In CTR encryption, the forward cipher function is invoked on each counter block, and the resulting output blocks are exclusive-ORed with the corresponding plaintext blocks to produce the ciphertext blocks. For the last block, which may be a partial block of u bits, the most significant u bits of the last output block are used for the exclusive-OR operation; the remaining b-u bits of the last output block are discarded.

CTR Encryption:

$$O_j = CIPH_K(T_j) \quad \text{for } j = 1, 2 \ldots n;$$
$$C_j = P_j \oplus O_j \quad \text{for } j = 1, 2 \ldots n\text{-}1;$$
$$C_n^* = P_n^* \oplus MSB_u(O_n).$$

CTR Decryption:

$$O_j = CIPH_K(T_j) \quad \text{for } j = 1, 2 \ldots n;$$
$$P_j = C_j \oplus O_j \quad \text{for } j = 1, 2 \ldots n\text{-}1;$$
$$P_n^* = C_n^* \oplus MSB_u(O_n).$$

In CTR decryption, the forward cipher function is invoked on each counter block, and the resulting output blocks are exclusive-ORed with the corresponding ciphertext blocks to recover the plaintext blocks. For the last block, which may be a partial block of u bits, the most significant u bits of the last output block are used for the exclusive-OR operation; the remaining b-u bits of the last output block are discarded.

3. Security of a cipher:

The level of security against cryptanalysis may be measured as the amount of work (computations) required by the adversary to break the cipher. Ideally, a computationally secure encryption system would make it impossible to break the cipher with an exhaustive search approach having exponential order complexity. Nevertheless, practical encryption systems may have vulnerabilities leading to possible short cut attacks making it possible to break the cipher with algorithms of complexities less than an exponential order. Meanwhile, it is reasonable to say that there is no such thing as a completely secure encryption system, and the level of security can only be quantified relative to the strength of the adversary present in the environment. It is possible to model the adversary's "strength" to break a cipher as a random parameter using a probability distribution. It is reasonable to assume that the ability of the adversary to break the cipher becomes less probable as the key length, block length, diffusion, and so forth, increase.

Need of One Key per Block Length

If a common key were to be used for all the block lengths, then an attack on the smaller block length would reveal a part of the key. After a part of the key is revealed, increasing the lock length would not exponentially increase the security of the cipher. Since keys are changed only once in every session and thousands of encryption operations are performed before each key change, we expect minimal impact on the complexity of key management due to our requirement of having a separate encryption key per block length.

4. Exploits to defeat security in wireless communicatiton: wep security flaws

There exist several exploits in the security of WEP resulting in breakable system and leaving it fragile and unreliable. In order to identify these problems we first need to understand how WEP intends to achieve its goals. WEP relies on an encryption algorithm called RC4. This algorithm works as follows:

Packet injection

Packet injection is sometimes understood as not a real attack on WEP, because WEP was never designed to be resistant against such an attack. A packet sent in a WEP protected network which has been intercepted by an attacker, can later be injected into the network again, as long as the key has not been changed and the original sending station is still in the network. If the sending station is not in the network anymore, the senders (and the receivers) address can be changed to a station that is still in the network. This is possible, because these fields are not protected by the ICV.

Fake authentication

The fake authentication attack on the WEP protocol allows an attacker to join a WEP protected network, even if the attacker has not got the secret root key. IEEE 802.11 defines two ways a client can authenticate itself in a WEP protected environment.

KoreK's chopchop attack

KoreK's chopchop attack is quite an remarkable attack on WEP. As summarized: Let Ocrc be an oracle, which takes an arbitrary encrypted packet and returns true, if the checksum in the encrypted packet was correct, false otherwise. If an attacker has a single encrypted packet of length l and access to such an oracle Ocrc, he can decrypt the last m bytes of the packet and recover the last m bytes of the key stream used to encrypt the packet, with in average 128 x m queries to the oracle and negligible computational effort.

Arbaugh inductive attack

In a nutshell, Arbaugh could show the following: If an attacker has recovered a single encrypted packet of length l and has access to Ocrc, he can determine the next m bytes of the key stream used to encrypt this packet with in average m x 128 queries to the oracle and negligible computational effort.

5. Evaluated security mechanisms: wep (wired equivalent privacy)

The WEP allows the manager to create several passwords and share them with wireless network users. In this case, the passwords sequences are created by the cryptography algorithm WEP. The algorithm method used by WEP, is RC4 with keys of 64 to 256 bits [4]. When a station receives a package without the cryptography, with the key created by the manager, the package is automatically discarded, preventing unauthorized users from having access to the network. Another option to WEP security is the joint use with the filter of MAC addresses of each user in the access configuration. Besides the password cryptography, the user without a registered MAC address cannot have access to access point, which avoids unknown user's infiltration. Figure 2 introduces the cryptography process developed by the WEP mechanism, when control of the key is the critical point to keeping safe access to the network.

WPA (WiFi Protected Access)

The WPA came with the purpose of solving the problems in the WEP cryptography method, without the user's needs to change the hardware. The WPA-PSK is a network authentication which does not use an authentication server and the data cryptography key can go up to 256 bits. The WPA allows a more complex data cryptography based on the TKIP protocol (Temporal Key Integrity Protocol), being also assisted by MIC Message Integrity Check), which function is to avoid attacks of bit-flipping type easily applied to WEP who uses a hashing technique [8].

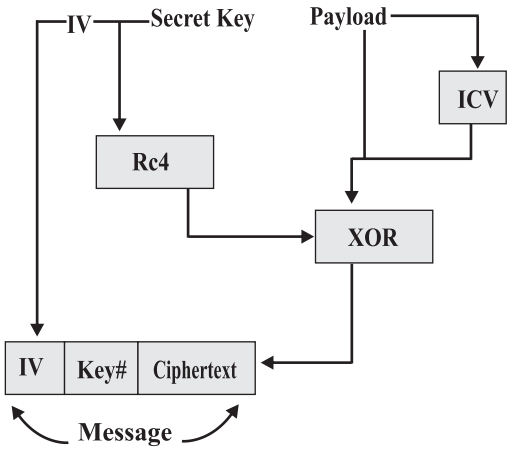

Fig.2. WEP Cryptography process.

In the generation of the cryptography, the TKIP uses the same WEP's Technique (RC4), making a hash before the increasing of the algorithm RC4. A duplication of the initialization vector is made. One copy is sent to the next step, and the other is hashed (mixed) with the base key. After accomplishing the hashing, the result generates the key to the package that is going to join the first copy of the initialization vector, occurring the increment of the algorithm RC4. After that, there's the generation of a sequential key with an open XOR from the text that you wish to cryptograph, generating then the cryptography text. Its decryptography is accomplished by inverting the process.

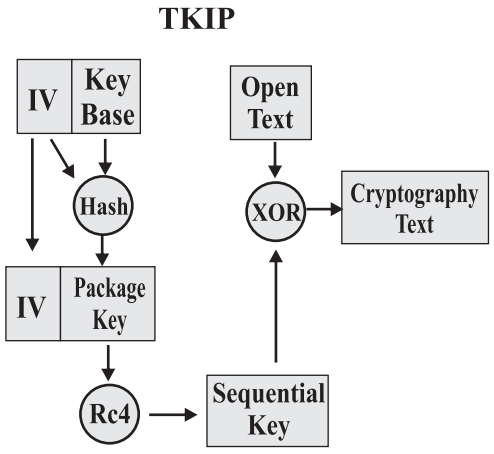

Fig.3. WPA Cryptography process

6. Elements of performance:

Response time

The time that a package takes to transit between two points (transmitter and receiver). It shows how the Network applications seem to work. A slow answer (high response time) is enlarged by applications that need to transmit lots of data by the network or by applications, which produce immediate results from a client's input.

Utilization

The utilization of the network represents a percentage of time when the network was in use in a specific period. The calculation requires sent and received data information, value of the interface and time of evaluation.

Throughput

Throughput is the bytes quantity transmitted in a certain time, being the bandwidth available for an application at any time. The networks 802.11 use the access protocol CSMA/AC which uses an ACK (Acknowledge) positive recognition. When a client receives a package, he answers with an ACK, in case that ACK does not return to the client who sent the package, it is taken over that the package was lost, causing an overhead [5, 6].

7. Results:

Based on network of the figure 5, the experiences were initiated by measuring the throughput and response time to the TCP and UDP protocols in the 802.11g network, with a wireless station associated (figure 6) [7]. To the TCP traffic the WEP 128 bits security mechanism decreased the through put in 20%, the WEP 64 in 14% and the WPA in 14 %.

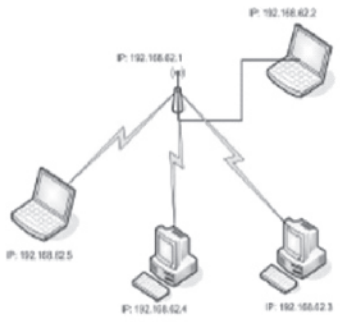

Figure 4. Tests scenario.

Using UDP traffic the biggest throughput drop happened with the WEP's 128 bits utilization, 7% less regarding the tests without security. The response time for each test is shown in table 1.

Table 1Response time in milliseconds/one connection

1 Station	TCP	UPD
Without Cryptography	7	5
WEP 64	8	8
WEP 128	9	8
WPA	8	8

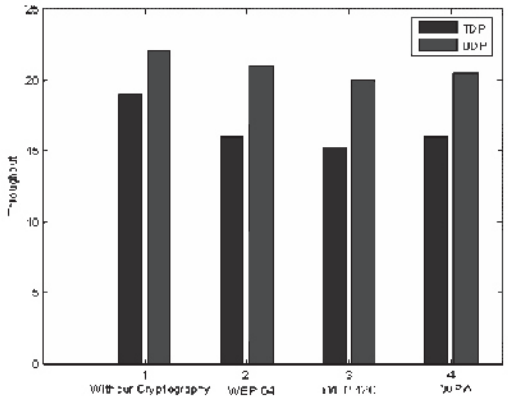

Figure 5. Throughput for a station Wireless associate to AP

2 Station	TCP	UPD
Without Cryptography	13	16
WEP 64	16	17
WEP 128	16	17
WPA	16	17

Table 2 Response time in milliseconds/one connection

2 Station	TCP	UPD
Without Cryptography	19	23
WEP 64	22	28
WEP 128	23	24
WPA	21	28

Table 3Response time in MS to 3 wireless stations of AP

After associating the third wireless station the average decrease of throughput in TCP traffic was 64% and 32% regarding the two stations (figure 6). For UDP was respectively 66% and 30% can be observed in table 3.

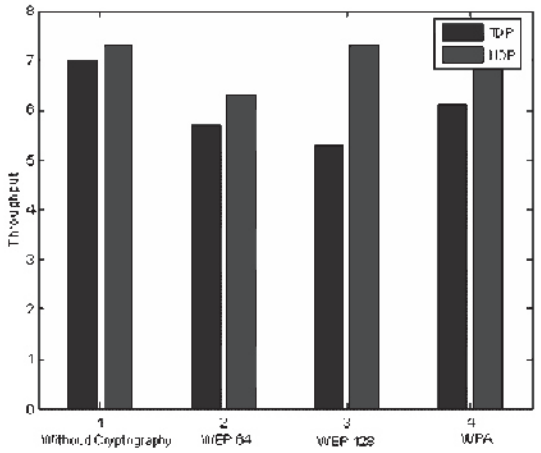

Figure 6. Throughput for three wireless stations associates to AP

8.conclusions:

The overload inserted in the wireless network IEEE 802.11g by the security methods WEP 64, WEP 128 and WPA is studied. Also it is been realized that how the encryption based on wireless channel states could lead to significant gains in the throughput achieved for a specified security constraint. As is observed, the WPA seems to correct the WEP failures introduces, and according to the accomplished tests, introducing a better performance than its predecessor.

9. References:

[1] Baghaei, Nilufar: IEEE 802.11 Wireless LAN Security Performance Using Multiple Clients, 2003.

[2] Maciel Junior, Paulo Ditarso; Astuto Arouche Nunes, Bruno Vieira; Campos; Carlos Alberto; Magalhaesde Moraes, Luis Felipe: Avaliando a Sobrecarga Introduzida nas Redes 802.11 pelos Mecanismos de Seguranca WEP e VPN/IPSec, 2003.

[3] W.C. Jakes, Microwave Mobile Communications. IEEE, 1974.

[4] Cisco Systems, AWLF: Aironet Wireless LAN Fundamentals student guide, Volume 1, Versao 3.1, Editora Cisco Systems, 2003.

[5] Blum, Richard, Network: Performance Open Source Toolkit, Ia Edicao, Editora Wiley, 2003.

[6] Akin, Devin e Geier, Jim, CWAP: Certified Wireless Analysis Professional Official Study Guide, Ia Edicao, Editora McGraw Hill/Osborne, 2004.

[7] Duntemann's Jeff Jeff Duntemann's: Drive-By Wi-Fi Guide, 2003.