A Light Weight Enhancement to RC4 Based Security for Resource Constrained Wireless Devices

Chetan Nanjunda Mathur and K. P. Subbalakshmi
(Corresponding author: Chetan Nanjunda Mathur)

Media Security, Networking and Communications Lab,
208 Burchard, Electrical and Computer Engineering Department,
Stevens Institute of Technology, Castle Point on Hudson, Hoboken, New Jersey 07030, USA

(Received Dec. 9, 2005; revised and accepted Feb. 21, 2006)

Abstract

The Wired Equivalent Privacy (WEP) uses the 64 bit RC4 secret key stream cipher as its layer 2 security protocol. Although the underlying RC4 cipher is secure, the potential reuse of the same key stream by different frames is a weakness in the WEP. One enhancement to WEP is the Temporal Key Integrity Protocol (TKIP), which acts as a wrapper to the WEP protocol and uses a 128 bit RC4 encryption to eliminate the possibility of key reuse within a given session. However, TKIP cannot be gainfully employed in devices where the 64 bit RC4 encryption is hardwired. Also, with 128 bit encryption TKIP can secure 10^{30} frames per session. Comparing this to the typical number of frames per session (500-1000), it is easy to see that the use of a 128 bit key causes unnecessary drain of power. The Wifi Protected Access (WPA), uses a 128 bit Advanced Encryption Standard (AES) cipher in the Counter-Mode-CBC-MAC Protocol (CCMP). This protocol requires higher computational power than the TKIP and is only intended for devices which possess higher computational power and memory.

In this paper, we propose a light weight enhancement to the 64 bit WEP, which provides significant improvement in security (measured as the number of frames securely transmitted before base key change) with small energy and memory overhead. Moreover, our technique can be tailored to the specific needs of resource constrained environments to provide just the necessary level of security. We use the Intrinsyc CerfCube[1] as a resource constrained wireless device and measure the resource consumed by various wireless security protocols on this device. From the experimental results we see that proposed LWE consumes about 62% less power compared to TKIP and 99% less power compared CCMP (AES), while providing a security enhancement of 2^{32} over the WEP protocol. These results demonstrate the utility of LWE as a good security protocol for wireless networks with battery power constrained devices and systems where 64 bit WEP is hardwired.

Keywords: Light weight cryptography, RC4, stream cipher, TKIP, WEP, wireless security

1 Introduction

The current security standard for wireless LANs (WLANs) is the wired equivalent privacy (WEP) [13]. The main aim of the WEP is to protect WLANs from eavesdropping and unauthorized access. The WEP employs the RC4 [15] encryption algorithm as its layer 2 cipher. The RC4 algorithm uses a base key to generate a key stream which is then XORed with the frame. To supply different keys for each frame, a 24 bit initialization vector (IV) is used to construct a per-frame RC4 key. The IV starts with a fixed value and increments every time a frame is encrypted. Once the IV space gets exhausted, the IVs are reused. The reuse of IVs results in the repetition of the key stream generated by the RC4 encryption algorithm leading to vulnerability against known plain text type attacks. In fact, this weakness has been exploited in [8], also known as the Fluhrer Martin Shamir (FMS) attack, where the cipher was cracked within a few minutes using packet flooding and birthday attack [22]. The packet flooding made the reuse of the same IV highly probable which was then modeled as a birthday attack to detect the duplicate IVs.

Several researchers have since proposed security enhancements to the WEP. The temporal key integrity protocol (TKIP) [19] uses a 128 bit key and rapidly changes the base key used by the RC4 cipher. The main aim here is to minimize the repetition of the key stream and hence to make it difficult for an adversary to attack the

[1] http://www.intrinsyc.com/products/mob_ref_sys/cerfcube_255/

system. However, this technique adds significant computational overhead to the WEP based systems. Another approach to enhance the security for WLANs is to replace the layer 2 security protocol, the RC4, with a strong block cipher. One of the most widely used symmetric block cipher for wired networks is the Advanced Encryption Standard (AES) [7]. There have been no practical attacks on AES until now and hence it is one of the contenders as a long term security solution for WLANs. The IEEE 802.11i recommends the use of AES in Counter-mode-CBC-MAC Protocol (CCMP). The hardware and processing power required by AES exceeds the capacity of most of the currently deployed wireless platforms. Hence, there is much research being done to make the CCMP energy efficient [11] and/or develop new lightweight security mechanisms that can work on existing platforms.

In this paper, we present our light weight enhancement to the WEP, that trades-off between power, memory and security. Our approach is based on derangement (special case of permutation) and complementation. The uniqueness of our approach is that we use the block cipher mode of operation on top of a 64-bit RC4 stream cipher to enhance the security. Although, block ciphers can exhibit channel error propagation [12], we avoid this drawback in the proposed algorithm by using a permutation-complementation based cipher which are known to be "error preserving" [18]. Further, the common drawback of error preserving ciphers (vulnerability to plaintext attacks) is avoided by using the proposed algorithm as a wrapper on the stream cipher based WEP. Hence, the proposed algorithm is able to provide security enhancements without causing error propagation.

Moreover, our proposed technique offers flexibility in security by giving the ability to control the number of frames securely transmitted before encryption key change. The power consumed by the 64-bit WEP, 128-bit TKIP, 128-bit CCMP and the proposed 64-bit light weight enhanced WEP (LWE) protocols were measured on a resource constrained Intrinsyc CerfCube (233MHz ARM processor, 16MB flash and 32MB SDRAM) and it was seen that the proposed LWE consumes about 62% less power compared to TKIP and 99% less power compared CCMP, while providing a security enhancement of 2^{32} over the WEP protocol. Finally, we conclude that LWE is ideal for use in wireless networks with battery power constrained devices and systems where 64 bit WEP is hardwired.

This rest of this paper is organized as follows. We present a brief overview of the WEP in Section 2 followed by a description of attacks on WEP in Section 3. Section 4 presents an overview of related work and the outline of error preserving function is given in Section 5. In Section 6 we describe the proposed enhancement to the WEP and discuss the tradeoff between power, memory and security. In Section 7 we present our experimental results and conclusion.

2 Overview of Wired Equivalent Privacy

As the name suggests, WEP goal was to create the level of privacy experienced on a wired LAN, in the wireless LAN. WEP uses a pre-established shared secret key called the base key, the RC4 [15] encryption and the cyclic redundancy check (CRC)-32 [4] checksum algorithms as its basic building blocks. It supports up to four different base keys, identified by KeyIDs 0 through 3. It selects a shared base key and a 24 bit initialization vector (IV) to construct a per-frame RC4 key by concatenating the IV value and the selected base key. The WEP then uses the per-frame key to RC4-encrypt both the data and the integrity check value (ICV), which are the parity check bits resulting from encoding the data using the CRC-32 code. The IV and KeyID identifying the selected key are encoded as a four-byte string and pre-pended to the encrypted data. The IEEE 802.11 standard defines the WEP base key size as consisting of either 40 or 104 bit, which when appended with the 24 bit IV becomes 64 and 128 bit respectively. At the time of the standard, most of the wireless devices could not afford 128 bit encryption, as a result 64 bit RC4 encryption was hardwired into the wireless devices.

3 Attacks on WEP

As mentioned earlier, the main drawback in the design of the WEP is the reuse of IVs. An attacker can reduce the time required to see the reuse of an IV by generating a large number of frames using any application software like a web browser or email client and the 802.11a protocol (which has five times higher bandwidth). By generating numerous frames and using the fact that more than one user can access the wireless network, the attacker can apply the birthday paradox [14] to force the reuse of IVs within 10 minutes [21]. The attacker can now construct a table of IV and key-stream pairs using known plain texts. Once this table is constructed, the attacker does a simple lookup on the IV to get the key stream. XORing this key-stream with the captured cipher text gives the unknown plain text. The shortcomings in the WEP have been efficiently used to compromise its privacy goals with ease, regardless of the key size [1, 8, 17, 20].

4 Contemporary Security Enhancements of WEP

The WEP uses a 24-bit IV, which means that there can be no more than $2^{24} \simeq 16$ million per-frame keys associated with any base key. Existing enhancements to WEP can be roughly classified into schemes that replace the base key before the IVs are reused or schemes that replace the layer 2 cipher (RC4) with a stronger cipher.

4.1 WEP2/TKIP (Temporal Key Integrity Protocol)

The Temporal Key Integrity Protocol (TKIP) [19] is a suite of algorithms that acts as a wrapper on the WEP and is backward compatible with the WEP. This method replaces the base keys before the IVs are reused to enhance the security. It employs a per-frame key construction, called the TKIP key mixing function which substitutes a 128 bit temporal key [9] for the WEP base key and constructs the WEP per-frame key using a tiny cipher [19]. Temporal keys are so named because they have a fixed lifetime and are replaced frequently.

The TKIP key mixing function can construct at most 2^{16} IVs after which, a rekeying mechanism provides fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse. The security enhancement aimed by TKIP is only viable when 128 RC4 encryption is used. Although TKIP is compatible with systems where 64 bit RC4 encryption is hardwired, there is no significant security enhancement provided by these systems.

4.2 AES (Advanced Encryption Standard)

One of the most widely used symmetric cipher for wired networks is the Advanced Encryption Standard (AES) [7] which is based on the Rijndael algorithm proposed by Daemen and Rijmen [5]. There have been no practical attacks on AES until now and for this reason, it has been thought of as a long term solution to the encryption standard for WLANs. The AES has variable block and key lengths: 128-, 192- and 256-bit. The block and key lengths for this algorithm can easily be extended to multiples of 32 bit, and works well across different processors, hardware and software.

Unfortunately, like many cryptographically strong ciphers, AES exhibits completeness (every cipher text bit depends on all the plain text bits) and hence the avalanche effect (a single bit flip in cipher text will cause one half of the bits to be flipped in the recovered plain text) [10, 6]. As wireless channels are prone to errors, incorporating AES as the layer 2 cipher in WLANs could potentially lead to the need for strong error correcting codes [4] and/or excessive retransmissions. Hence, the 802.11i recommends to use the AES in a stream cipher mode in the Counter-Mode-CBC-MAC protocol (CCMP). In this mode, one bit flip in the encrypted message during transmission causes only one bit flip after decryption at the receiver. The CCMP is thought of as a long term solution that addresses all known WEP deficiencies, but without considering the currently deployed hardware limitations [3].

Considering the limitations on bandwidth, processing resources and power in a wireless network, AES is not a feasible replacement as the layer 2 cipher for resource constrained environments.

5 Error Preserving Encryption Algorithms

One way to deal with the problem of error propagation is to use distance preserving encryption techniques. In [18] the authors present error preserving encryption functions for wireless networks that use operations like permutation and complementation to cause diffusion and confusion [16], which are the two basic building blocks of a cryptographic system. The aim here is to provide security without introducing error propagation. The cryptographic transformations in the error preserving functions generate a one to one mapping between the plain text and the cipher text bits thus violating the property of completeness. It has also been shown that for n-bit messages the number of error preserving functions is $n!2^n$ and that *all error-preserving functions can be generated using permutation and complementation operations* [18]. Although, error preserving encryption systems provide a huge key space, they cannot be used directly to secure a wireless system. This is because, error preserving encryption techniques are vulnerable to known plaintext attacks (described in the following section). However, in our proposed LWE protocol, we use error preserving encryption as a wrapper over the 64-bit WEP, which makes resilient against known plaintext attacks.

5.1 A Known Plaintext Attack on Error Preserving Encryption

A known plain text attack on the error preserving encryption technique is described in [18]. Here the attacker uses both the known message and its encrypted version to decode another encrypted message. Consider an example where the adversary is given a cipher text C_1 and must determine the corresponding plain text P_1 without querying the decryption function. The adversary then performs the following operations

- queries the encryption function for known plaintext P_2, to get the corresponding ciphertext C_2
- evaluates the Hamming distance d_2 between the ciphertext C_1 and the known ciphertext C_2. Due to the distance preserving property of the permutation-complementation based ciphers, the Hamming distance between the unknown plain text P_1 and the known plaintext P_2, is also d_2
- For n bit blocks, P_1 could be any one of the $\binom{n}{d_2}n$ bit strings that are at a Hamming distance of d_2 from the known plaintext P_2. Thus the adversary only has to search a subset of n dimensional vectors to find the plaintext P_1. Let η be the subset in which P_1 exits.
- The adversary performs the above operations on known plaintexts P_3,P_4.. until η contains only one element. This element is P_1.

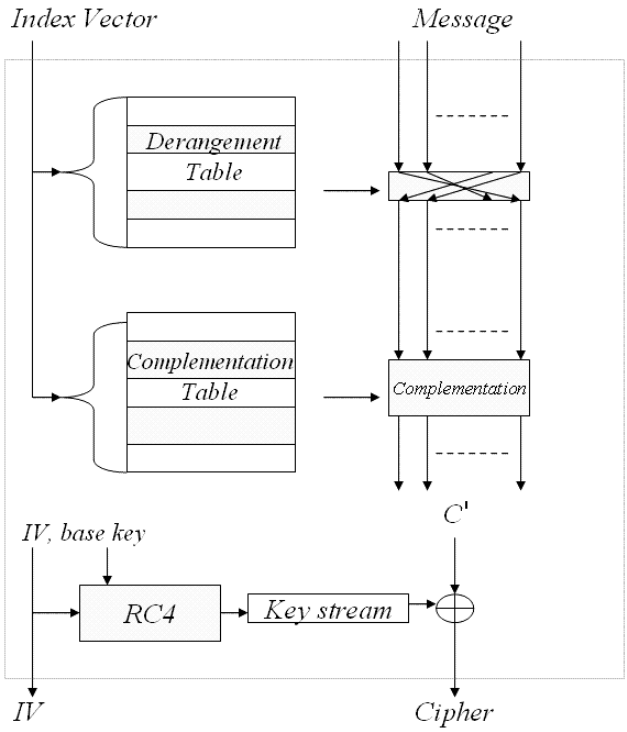

Figure 1: Block diagram of the proposed LWE scheme

6 The Proposed Light Weight Enhancement to RC4

Motivated by the distance preserving property of permutations, we use derangements [2] (a special class of permutations) to cause diffusion. Derangements are permutations which map none of the bit to their original position. For example, the only derangements of $1, 2, 3$ are $2, 3, 1$ and $3, 1, 2$. The number of derangements, N_D, for a set of n bit is given by:

$$N_D = n! \left(1 + \frac{\sum_{i=1}^{n} (-1)^i}{i!}\right).$$

N_D converges to $\frac{n!}{e}$ as n tends to infinity. Confusion is caused by the complementation operation on the n bit deranged messages. The total number of complements for a set of n bit, N_C, is 2^n. The number of ways to select a derangement and a complementation pair for a set of n bit is $N_D N_C$. We propose to enhance the security of the WEP and at the same time provide a means of trading off power and memory by combining error preserving functions with the RC4 cipher.

Figure 1 describes our encryption technique which operates on $n-$bit blocks of messages at a time. We have a N_{dc}-row derangement table, with $N_{dc} \leq N_D$, where each row represents a derangement vector for n bit.

The complementation table also contains N_{dc} rows, with $N_{dc} \leq N_C$, where each row represents one complementation vector for n bit. A Derangement-Complementation (D-C) pair is selected by indexing into the respective tables with an index value i contained in the index vector. The size of the index vector is $\log_2 N_{dc}$. The index starts with a fixed value between 1 and N_{dc} and remains the same until the IVs get exhausted. The index vector increments by one ($i_{\text{new}} = (i + 1) \text{mod} N_{dc}$) every time the IV gets exhausted. Since the IV is 24 bit long, this takes about 2^{24} frame transmissions. The message is first deranged and then complemented to get the intermediate cipher text, C'. The key stream generated by the RC4 [15] encryption is XORed with C' to get the final cipher. This along with the IV and index vector is then transmitted by the sender. The decryption process is essentially the reverse of the encryption process. The number of bit required to represent one derangement of n positions is $n \log_2 n$. The number of bit required to represent one complementation of n positions is n. Therefore, the total memory required to store the D-C tables of N_{dc} rows is $N_{dc}(n(\log_2 n + 1))$ bit. A base key exchange takes place after the index vector gets exhausted. Notice that, the interval between base key exchange now depends on the lengths of the index vector and the initialization vector (IV). This implies that a larger index vector (size of D-C table) results in exponentially longer interval between base key exchanges. Whereas, in the WEP the interval between base key exchange depended only on the length of IV and thus has limited flexibility.

6.1 Effect of Channel Errors

The D-C operations are distance preserving. The RC4 encryption algorithm XORs the message with the key stream. The XOR operations, in themselves do not propagate bit errors. Hence when combined, the RC4 and the D-C operations do not lead to error propagation. That is, the number of bit errors that occur in the channel remain the same after decryption, unlike in AES. Hence, this type of encryption technique is well suited for wireless networks.

6.2 Enhancement in Security

The security of WEP can be quantified as the number of frames that can be securely transmitted before base key change is necessary. As demonstrated in Section 3, the RC4 encryption as used in WEP can be considered secure until the IV, base key pair are not reused. There are 2^{24} different IV's for a given base key; hence, the security of RC4 is 2^{24}. For the proposed LWE mechanism the same IV, base key and index vector (or a row in the DC table) combination results is a one to one mapping between the plain texts and the corresponding cipher texts. Such a system can be broken by the known plain text attack that was described in Section 5.1. We calculated the number of plain text, cipher text pairs required to crack the unknown plain text with complete certainty. We found that for the best case (for the attacker), only three plain text-cipher text pairs are required. Therefore a base key change is required after every IV, index vector pair is used at most

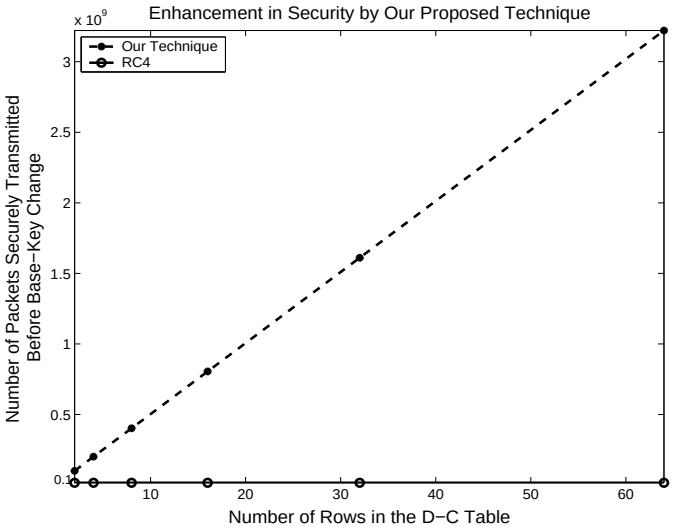

Figure 2: Enhancement in security due to the proposed LWE for a 128 bit message length and 104 bit RC4 base key

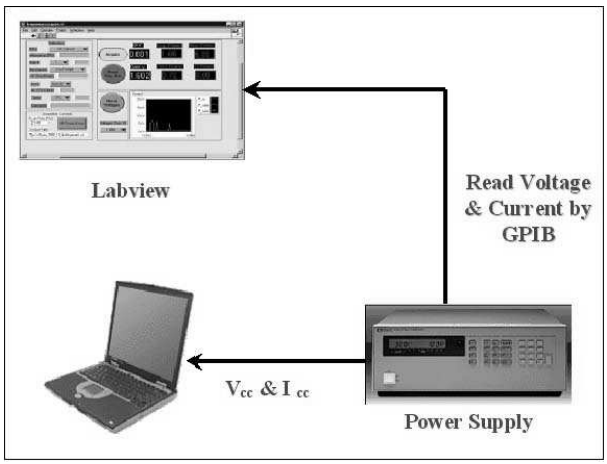

Figure 3: Hardware Setup

thrice. If security is quantified as the number of frames that can be securely transmitted before the need for a base key change, the security of LWE is $2^{24} \times 3N_{dc}$, where N_{dc} is the number of rows in the D-C table. This quantity can be equivalently expressed as $2^{24+\log_2 N_{dc}+\log_2 3}$. The security provided by the RC4 cipher on the other hand, is 2^{24}. Figure 2 plots (in log scale) the graph of the number of frames that can be transmitted before a mandatory key change versus the number of rows in the D- and C-tables, for a 128-bit message and 104-bit RC4 base key. As can be seen from this figure this number increases exponentially with increase in the number of entries in the tables.

7 Experimental Results and Conclusion

Two sets of experiments were conducted, one on a laptop and one on the Intrinsyc CerfCube. The CerfCube represents an environment with severe battery power and computational resource constraints and the laptop represents an environment in which the resource constraints can be relaxed. The test bed (Figure 3) consists of a Sony Vaio laptop with a 1.8 GHz intel P-4 processor, 512 MB RAM, running Red Hat Linux 2.4.8 and a Intrinsyc CerfCube with a 233 MHz ARM processor, 16MB Flash and 32MB SDRAM, running Debian linux operating system.

The power consumed by the CPU in running the encryption algorithms is measured as a function of input power supply to the Laptop/CerfCube. A separate DC power supply is given to the Laptop/CerfCube to permit measurements. The battery of the laptop is removed for accuracy in measurements. The current is measured using Labview from the GPIB interface of the power supply. To eliminate effects of any programs running in the background, the current consumption is first tested when no other tasks are running. The difference in currents when the algorithm is running and the idle current (in Amperes) is taken as the actual current consumption. In the experiments, since voltage variation is seen to be extremely small (measured to be less than 0.025%) we use a constant value. We use OProfile[2] to measure the exact time taken by the algorithms to run. The energy consumed by the algorithms is the product of power drawn from the DC source and the time required to complete execution.

7.1 Energy Consumption by Our Proposed Technique

We measure the energy consumption of our proposed light weight mechanism and compare it with the energy consumption of the WEP, TKIP and the AES-CCM protocols. The WEP and light weight enhanced WEP use RC4 in 64 bit encryption mode, whereas the TKIP uses RC4 in 128 bit encryption mode. The AES-CCM uses the AES block cipher in 128 bit encryption mode. We conducted two sets of experiment to measure energy consumed by our proposed light weight mechanism. The first set of experiment was performed on the laptop, where we measure the energy consumed to encrypt one frame (256 bytes). This gives us an average sense of energy consumption by different encryption algorithms. In the second set of experiment, we used the CerfCube which has limited computational and memory resources. Here we measured the peak energy consumption per encryption by different algorithms. This gives us the minimum energy requirement for resource constrained devices to support different encryption algorithms. The results are briefly summarized below:

- *Energy consumption per frame*: We calculated the energy consumed by our proposed light weight en-

[2]http://oprofile.sourceforge.net

hanced WEP (LWE) for different sizes of the D-C table, the WEP and the TKIP protocols on the laptop. Figure 4 plots the energy consumed per 256 bytes frame by these protocols against the number of bit used to index the entries of the D-C table (equivalent to the log of the number of rows). Note that the size of the D-C table is only relevant to our proposed technique. We can observe from the figure that TKIP consumes on an average about 90% more energy compared to WEP. On the other hand, light weight enhanced WEP (with 256 rows in D-C table or 8 bit index) is practically a light weight enhancement with only about 25% increase in energy consumption and improvement in the security of about 2^{32} frames compared to the WEP.

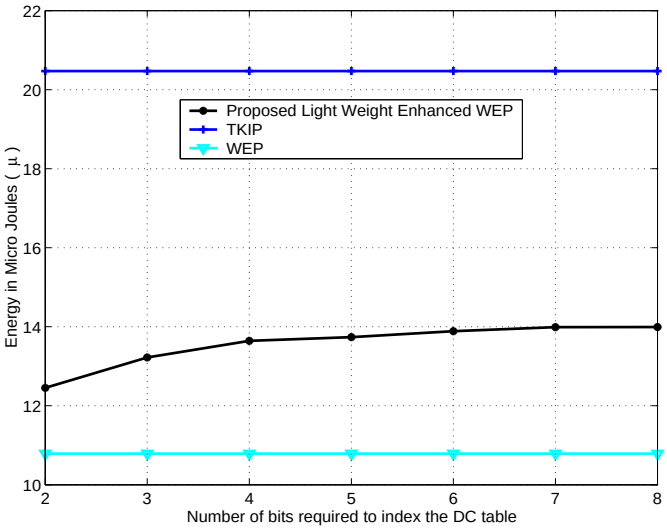

Figure 4: Energy consumption per 256 bytes frame by WEP, TKIP, and the proposed light weight enhanced WEP against different sizes of the D-C table used in our proposed technique.

- *Peak energy consumption per encryption*: We calculated the peak energy consumption of LWE, WEP, TKIP and AES-CCM on the CerfCube. Figure 5 plots the energy consumption per encryption for these protocols. It can be observed that the proposed LWE consumes about 62% less power compared to TKIP and 99% less power compared CCMP, while providing a security enhancement of 2^{32} over the WEP protocol. Also, notice that AES-CCM has the highest peak energy consumption and the WEP has the lowest peak energy consumption suggesting that increase in security is related to increase in energy consumption. Our proposed Light Weight Enhancement approach allows us to tradeoff this energy-security optimization.

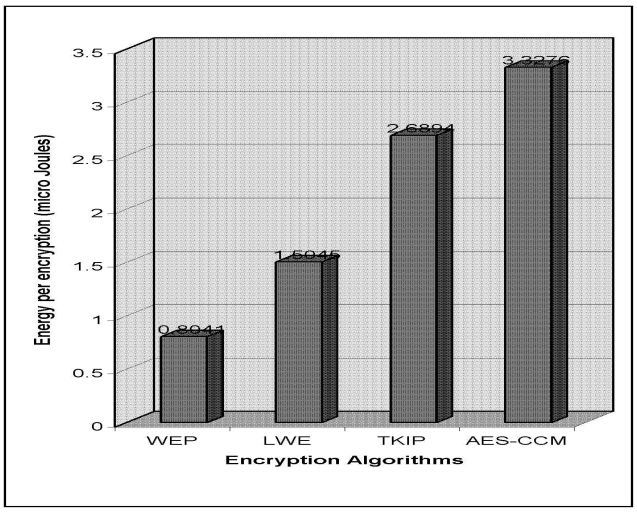

Figure 5: Energy consumption per encryption by WEP, TKIP, proposed Light Weight Enhanced WEP (LWE) and AES-CCM protocol.

8 Conclusions

We studied the contemporary approaches to wireless network security at the link layer. It was observed that for wireless networks with resource constrained devices 128 bit encryption provided by TKIP and CCMP over allocate security. The design of light weight enhancement for the 64 bit WEP was proposed. The security improvement due to LWE was quantified as the number of frames that can be securely transmitted before base key change. Security analysis showed that this system gives the user the flexibility to incrementally trade computation and memory for exponential improvements in security. Experiments revealed that a) using LWE we can exponentially increase security (2^{32} frames) with logarithmic expenditure of memory and power (25%) b) LWE consumes about 62% less power compared to TKIP and 99% less power compared CCMP. Hence, LWE is ideal for use in wireless networks with battery powered or resource constrained devices and systems where 64 bit WEP is hardwired.

Acknowledgements

We have to acknowledge the following: US Army ARDEC/Picatinny arsenal.

References

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom'01)*, pp. 180-189, ACM Press, New York, NY, USA, 2001.

[2] R. A. Brualdi, *Introductory Combinatorics*, Prentice Hall, 1999.

[3] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," *Communications of ACM*, vol. 46, no. 5, pp. 35-39, 2003.

[4] X. Chen, *Error-Control Coding for Data Networks*. Kluwer Academic Publishers, Norwell, MA, USA, 1999.

[5] J. Daemen and V. Rijmen, *The design of Rijndael: AES — the Advanced Encryption Standard*, Springer-Verlag, 2002.

[6] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, no. 5, pp. 15-23, May 1973.

[7] FIPS, *Specification for the Advanced Encryption Standard (aes)*, Federal Information Processing Standards Publication 197, 2001.

[8] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," in *Selected Areas in Cryptography 2001*, LNCS 2259, pp. 1-24, Springer-Verlag, 2001.

[9] R. Housely and D. Whiting, *Temporal Key Hash*, IEEE 802.11 doc 01-550r1, Oct. 2001.

[10] J. B. Kam and G. I. Davida, "Structured design of substitution-permutation encryption networks," *IEEE Transactions on Computers*, vol. 28, no. 10, pp. 747-753, 1979.

[11] C. N. Mathur, K. Narayan, and K. Subbalakshmi, "High diffusion cipher: Encryption and error correction in a single cryptographic primitive," in *4th International Conference on Applied Cryptography and Network Security Conference (ACNS)*, pp. 309-324, June 2006.

[12] C. Nanjunda, M. Haleem, and R. Chandramouli, "Robust encryption for secure image transmission over wireless channels," in *IEEE International Conference on Communications (ICC'05)*, vol. 2, pp. 1287-1291, Seoul, Korea, May 16-20, 2005.

[13] IEEE Computer Society, *Wireless Lan Medium Access Control (MAC) and Physical Layer (PHY) specifications*, part 11, 1999.

[14] S. Ross, *A First Course in Probability*. Macmillan, 3rd Edition, 1988.

[15] B. Schneier, *Applied Cryptography (2nd Edition): Protocols, Algorithms, and Source Code in C*, John Wiley & Sons, Inc., New York, NY, USA, 1995.

[16] C. E. Shannon, "Communication theory of secrecy systems," *Bell Systems Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[17] A. Stubblefield, J. Ioannidis, and A. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break Wep*, ATT Labs Technical Report, TD4ZCPZZ, Revision 2, Aug. 21, 2001.

[18] A. S. Tosun and W. chi Feng, "On error preserving encryption algorithms for wireless video transmission," in *Proceedings of The Ninth ACM International Conference on Multimedia (MULTIMEDIA'01)*, pp. 302-308, ACM Press, New York, NY, USA, 2001.

[19] J. Walker, *802.11 Security Series Part II: The Temporal Key Integrity Protocol (TKIP)*, Technical report, Platform Networking Group, Intel Corporation.

[20] J. Walker, *IEEE p802.11 Wireless Lans Unsafe at any Key Size; An Analysis of the Wep Encapsulation*, Technical report, Platform Networking Group, Intel Corporation, Oct. 2000.

[21] C. D. J. Welch and M. S. D. Lathrop, *A Survey of 802.11a Wireless Security Threats and Security Mechanisms*, Technical Report ITOC-TR-2003-101, Department of Electrical Engineering and Computer Science, United States Military Academy at West Point, West Point, New York, 2003.

[22] G. Yuval, "How to swindle Rabin," *Cryptologia*, vol. 3, no. 3, pp. 187-189, july 1979.

Chetan Nanjunda Mathur is currently pursuing his Ph.D. in Computer Engineering at Stevens Institute of Technology, New Jersey, USA. He was born in Bangalore, India in 1981. He received his BE degree in Computer Science from Visveshwaraiah Institute of Technology, Bangalore, India in 2002. He has an MS in Computer Engineering from Stevens Institute of Technology, New Jersey, USA. Part of Chetan's MS thesis was patented by Stevens Institute of Technology. In the past few years Chetan has published several research papers in the fields of Cryptography, Coding theory and Dynamic spectrum access. He has also received numerous awards including the IEEE best student paper award presented at IEEE Consumer Communications and Networking Conference (CCNC 2006) and the IEEE student travel grant award presented at International Conference on Communications (ICC 2005). He is an active student member of IEEE and is in the advisory board of Tau Beta Pi, the national organization of engineering excellence.

K. P. Subbalakshmi is an Assistant Professor in the Department of Electrical and Computer Engineering, Stevens Institute of Technology where she leads research projects in information security, encryption for wireless security, joint source-channel and distributed source-channel coding, with funding from the NSF, AFRL, ONR, US Army and other agencies. She is the Chair of the Security Special Internet Group of the IEEE Technical Committee on Multimedia Communications (MMTC) as well as the Secretary of the COMSOC MMTC. She was a Program Co-Chair of the IEEE GLOBECOM 2006, Symposium on Network and Information Security Systems. She served as a Guest Editor for the IEEE JSAC, Special Issue on Cross-Layer Optimized Wireless Multimedia Communication.