Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HARDWARE AND SOFTWARE IMPLEMENTATION FOR HIGHLY SECURED MODIFIED WIRED EQUIVALENT PRIVACY (MdWEP)

[1]M.VANITHA, [2]R.SELVAKUMAR, [3]S.SUBHA
[1]Asst. Professor (Sr), School of Information Technology and Engineering, VIT University, Vellore.
[2]Sr.Professor, School of Advanced Sciences, VIT University, Vellore
[3]Professor, School of Information Technology and Engineering, VIT University, Vellore.
E-mail: mvanitha@vit.ac.in, rselvakumar@vit.ac.in, ssubha@vit.ac.in

ABSTRACT

Wireless communication networks are in huge need and demand due to various features of internet and its availability and easy accessibility all over the world. Therefore, advanced security techniques and mechanism are required for private business application and for effective and secured data transfer from one network to other. Many common standards such as 6LoWPAN, Zigbee (IEEE 802.15.4-2006), WiFi (IEEE 802.11) and many more are being used for wireless standard. Many techniques used today having weak security and loop holes that can easily be attacked to gain access over the networks such as Wired Equivalent Privacy(WEP) can easily be stabbed with the ample availability of tools and the data present can be modified or read by the mediator. This paper aims for developing a Modified Wired Equivalent Privacy protocol (MdWEP) which will give more reliable communication and security benefits. To implement MdWEP we are using three cryptography algorithms AES, RSA and MD5. To increase the security three fold the plain text is passed through three cryptography architecture namely AES, RSA and MD5. Hardware implementation of this structure will consume more hardware and power but the speed can be increased by pipelining the output of each stage. Software implementation does not require huge resources but we get 3 times secured data. Hardware implementation is being done using xilinx and software implementation is being done by Java Swing

Keywords : *Zigbee, MdWEP, Wireless, IEEE 802.11, Hashing, Security*.

1. INTRODUCTION

The most important issue that arises now a day is to keep the mediators from accessing, modifying and reading the data present in the file while transmitting it from one network to other [1,2]. This algorithm approaches to provide security same as in wired network. In this paper we discussed how WEP works for wireless network and together with that it also explains what are the limitations and drawbacks.

The following algorithms are used in this paper to implement MdWEP:

RSA:- To Generate the digital Signature

AES:- To encrypt and decrypt the message.

MD:- To generate the message digest.

The paper has been organized as follows. Section 2 deals with the overview of WEP its operation and its drawbacks. Section 3 discusses the proposed Modified Wired Equivalent Privacy (MdWEP). Section 4, 5 and 6 discuss the MD5, RSA and AES algorithms respectively. Section 7 and 8 presents the hardware and software implementation results of proposed architecture and finally section 9 concludes the paper

2. WIRED EQUIVALENT PRIVACY (WEP)

As it name implies it provides security same as wired connection. It is a security algorithm for IEEE 802.11 [8] as its privacy component. It was designed specially to provide security in a wireless network as shown in figure.1.

2.1 Overview of WEP

The procedure for encryption of data frames with its description and analysis is given below

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The RC4 algorithm [3] is used to produce cipher text from plain text. XOR operation is performed between plain text and the ciphering key.

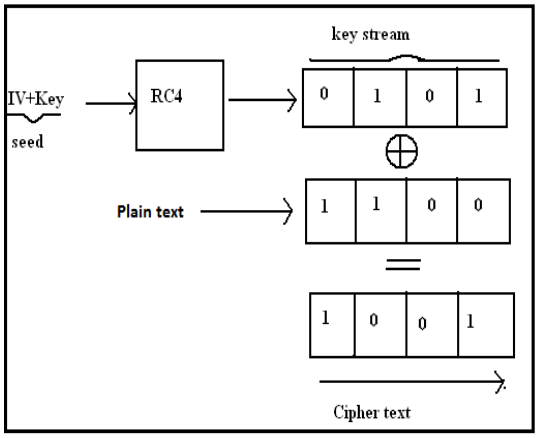

Figure.1 Encryption in WEP using RC4

2.2 Operation of WEP

The main goal of every cryptography algorithm is to encrypt and decrypt the message and the same is for WEP [4,8]. Encryption process involves converting the plain text to cipher text i.e. unreadable text and Decryption is just reverse of Encryption i.e. converting cipher text back into original text (plain text). Firstly, the plain text (denoted by pt) i.e. the original message which is send by the sender is converted into cipher text using any ciphering key. The data before decryption is cipher text (denoted by ct) which is converted into the plain text using the same ciphering key and the data after the decryption is plain text.

To produce the Output Text (ct) Encryption function (ef) will take (pt) as an input and produces the cipher text as shown in figure.2.

$$Ef(pt) = ct \quad (1)$$

In reverse process, the decryption function (df) will take (ct) as an input to produce (pt) as output.

$$Df(ct) = pt \quad (2)$$

The above all the equations and work can be summarized as following:

$$Df(ef(pt)) = pt \quad (3)$$

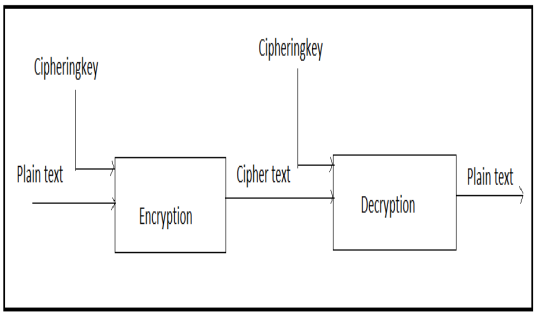

Figure.2 Encryption and Decryption Process

2.3. Drawbacks of WEP

In WEP encryption, any mediator or attacker can easily crack the key using any available software in less amount of time. It uses the single key for encryption of the message and the same key is transmitted towards the receiver side for decryption process [5], so in between the network if anyone get the key then he will easily breach the confidentiality.

Another drawback is that if there is need come to change the master key then the changes should be done every nodes connected to the network manually.

3. PROPOSED MODIFIED WIRED EQUIVALENT PRIVACY (MdWEP)

The main work of MdWEP is to enhance security between two communicating nodes over the network [6] is shown in figure 3. Here the process of encryption and decryption is explained which we have used in MdWEP i.e. how these both processes are done to achieve the goal of enhanced security. As discussed that RC4 algorithm [7] is used in WEP[10]s, In MdWEP the message digest using hash function (MD5) is generated firstly then digital signature is generated by using RSA using the sender's private key.

We used some symbols in the procedure of MdWEP, which are given below

S-sender, R-receiver , M-Message to be send, E1-encrypted message (generate using AES algorithm) E2 –encrpted hassh message H!,H2-hash code generated by MD5, K-Sender's public key, U-Sender's private key

3.1 Procedure

The procedure involved for implementing the MdWEP is explained below:

The following procedure is divided into two parts:

Sender Side:

Step1: The Sender S produces the message M that it has to send.

Step2: MD5 is used to produce hash code H1 by taking the Message M as Input.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Step3: RSA uses the senders public key K to encrypt the hash code H1
Step4: Message M is encrypted by using AES algorithm.
Step5: Now the message that is encrypted by AES in Step 4 is combined with the encrypted hash code produced in Step 3. The sender side illustration is shown in figure 3.

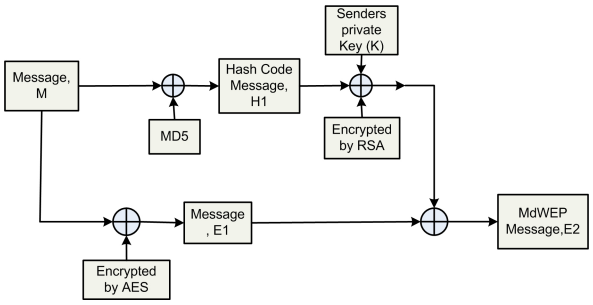

Figure.3 Block Diagram For Sender Side Mdwep

Receiver Side:
Step1: At the Receiver's end the receiver introduce RSA algorithm and uses sender's private key to decrypt the encrypted message i.e. H1 into H1 (only signature is decrypted)
Step2: After that AES is introduced to the encrypted message E2 for decryption
Step3: In this step use the output what we get in step 2, MD5 is introduced to generate hash code H2.
Step4: In this step we do the comparison of H1 and H2 if they are same then we give authentication to our message. The receiver side illustration is shown in figure 4.

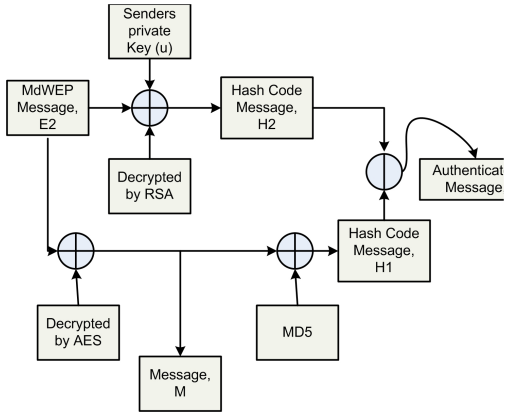

Figure.4 Block Diagram For Receiver Side Mdwep

4. MESSAGE DIGEST ALGORITHM (MD5)

In cryptography, Md5 algorithm is used to generate the hash. It generate 16byte hash code which is one of the best hash function used to check the data integrity and is represented as a 32-digit hexadecimal number.

4.1 Algorithm:

l: Padding is done in very first step i.e. padding re added to the original message. The goal of this nake original message of the length equal to a , i.e. 64-bits which is less than multiple of 512 bits own in the figure 5.

2: In this step we evaluate message original length ppend it to the end of the message.

3: Here the division of input message into block is each block of length 512-bits.

Step4: This step is also known as initializing chaining variables. In this four variables are given some initial hexadecimal values.

Step5: This step is quite complicated which is stated as follows:

- The value of four chaining variables is copied into four corresponding variables.
- Here 16 sub blocks have been created from the current 512-bits block, each block have 32-bits.
- In this step 32-bit word produced as output by taking the three 32-bit words from the following four functions. This processing is called as rounds. Based on modular addition, non-linear function (f) and left rotation each round has 16 operations.

  X (P, Q, R) = (P AND Q) OR (NOT (P) AND R)

  Y (P, Q, R) = (P AND R) OR (Q AND NOT(R))

  Z (P, Q, R) = P XOR Q XOR R

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

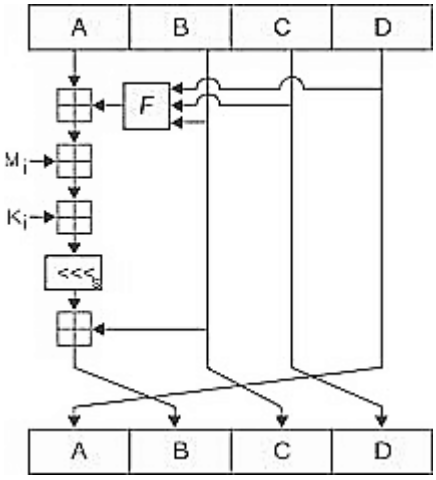

Figure.5 Illustration Of MD5 Operation

7. In the receiver side for decryption use cipher text CT to evaluate plain text PT
   $PT = CT^D \bmod N$

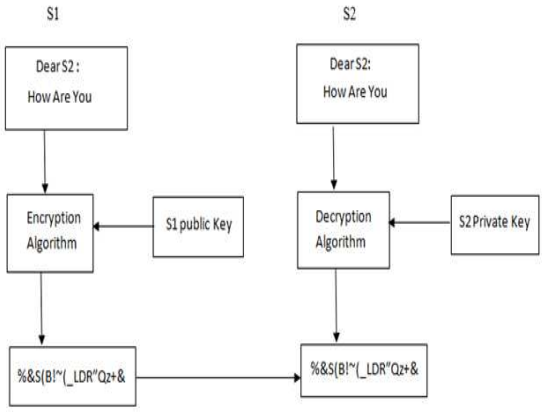

Figure.6 Illustration Of RSA Algorithm

5. RSA ALGORITHM

The RSA algorithm is a asymmetric key cryptographic algorithm. This algorithm as discussed above is asymmetric, requires public key for the creation of digital signature of the data. To decrypt that digital signature a private key is required by the receiver as shown in figure 6. For understanding this algorithm some basic knowledge of prime numbers as well as how to find the factors of any number is necessary.

The private and public keys in RSA are based on verge prime numbers (made up of 100 or more digits). The algorithm is simple but the real task arises in generation and selection of public and private keys

5.1 Operation

1. Select P and Q any two large prime numbers.
2. Evaluate N=P*Q
3. Now public key (i.e. encryption key) E is chosen in such a way that it should be not the factor of (Q-1) and (P-1).
4. For the selection of private key(i.e. decryption key) D in such a manner so that it satisfy the following equation:
   (D*E) mod (P-1)*(Q-1) = 1
5. Evaluate the cipher text CT from the plain text for encryption as follows :
   $CT = PT^E \bmod N$
6. Send to the receiver side CT as the cipher text.

6. AES (ADVANCED ENCRYPTION STANDARDS)

AES algorithm is an iterated block cipher supporting a variable data block and a variable key length of 128, 192 or 256 bits. The algorithm consists of three distinct phases [9], [11]-[13]: (i)an initial data/key addition, (ii) nine (128-bits), eleven (192-bits) or thirteen (256-bits) standard rounds, (iii) a final round which is a variation of a standard round. The number of standard rounds depends on the data block and key length. If the maximum length of the data block or key is 128, 192 or 256, then the number of rounds is 10, 12 or 14, respectively. The initial key is expanded to generate the round keys, each of size equal to block length. Each round of the algorithm receives a new round key from the key schedule module. Each standard round includes four fundamental algebraic function transformations on arrays of bytes. These transformations are: byte substitution, shift row, mix column, and round key addition as shown in figure 7. The final round of the algorithm is similar to the standard round, except that it does not have *MixColumn* operation. Decryption is performed by the application of the inverse transformations of the round functions. The sequence of operations for the standard round function differs from encryption. The computational performance differs between encryption and decryption because the inverse transformations in the round function is more complex than the corresponding transformation for encryption.

Journal of Theoretical and Applied Information Technology
20th February 2013. Vol. 48 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

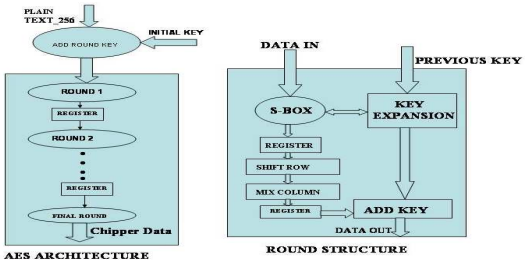

Figure.7 Illustration Of AES Algorithm

7. HARDWARE IMPLEMENTATION RESULTS

The hardware implementation of the algorithm is done using Verilog language for modelling and the simulation is done using modelsim and the synthesis is done using Xilinx XST synthesis targeting for Xilinx xc3s500e-4f8320 FPGA board. The synthesized RTL diagram is shown in the figure. 8. The simulated result is shown in figure 10. Figure 11 shows the resource utilization for FPGA implementation.

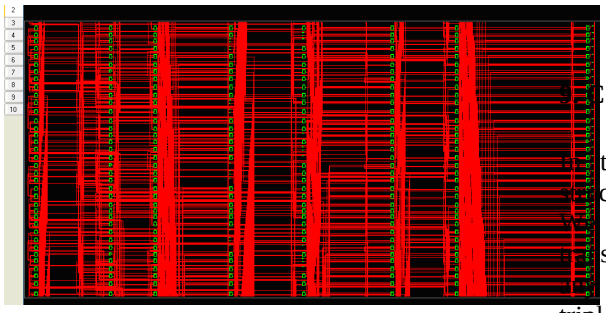

Fig.8 Synthesized RTL Diagram Of The Proposed Architecture

8. SOFTWARE IMPLEMENTATION RESULTS

The proposed algorithm is coded using Java swing and the simulation applet window snap shot is shown in figure 9.

Figure.9 Snap Shot Of MDWEP

ONCLUSION

this paper we have shown and explained the cture, architecture and implementation of MdWEP. have proposed a better and secured way for the smission of data over the network and also between two nodes in a network. Here we have proposed triple layer architecture of wi-fi security. Our technique is very much compatible with any hardware that supports WEP. Here confidentiality and integrity is provided to the data.

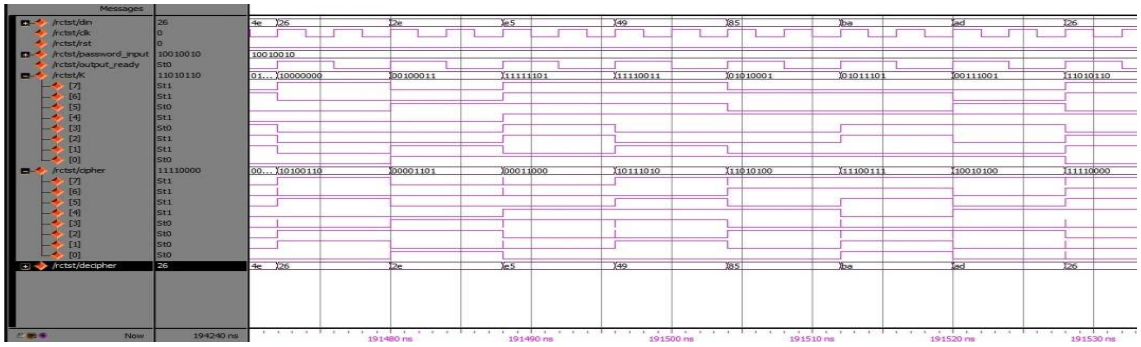

Figure.10 Simulation results of the proposed architecture

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Device Utilization Summary (estimated values)			
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	5409	4656	116%
Number of Slice Flip Flops	2179	9312	23%
Number of 4 input LUTs	9768	9312	104%
Number of bonded IOBs	43	232	18%
Number of GCLKs	1	24	4%

REFERENCES

[1] S Vinjosh Reddy, K Sai Ramani, K Rijutha Sk Moh Ali, CH. P Reddy, Wireless hacking - a WiFi hack by cracking WEP, *International Conference of Education Technology and Computer (ICETC)*, 2010.

[2]. 3GPP TS 33.401 v11.0.1. 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects. 3GPP System Architecture Evolution (SAE): Security Architecture. Release 11, June 2011.

[3] Ab. Al Noman, Dr Mohd Sidek R, Ramli, A, Ali L. Maskatani, RC4A stream cipher for WLAN security: A hardware approach, *International Conference on Electrical and Computer Engineering (ICECE)*, 2008.

[4] Laskari A.H, Mansook M, Danish A.S, Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA), *International Conference on Signal Processing Systems*, 2009.

[5] Hussain, H.R. Challal Y., Enhanced WEP: An effective solution to WEP throts, *Second IFIP International Conference*, 2005.

[6] Borsc, M., Shinde H, Wireless security & privacy, *IEEE International Conference on Personal Wireless Communications (ICPWC)*, 2005.

[7] Sourav Sen Gupta, Anupam Chattopadhyay, Koushik Sinha, Subhamoy Maitra, Bhabani P. Sinha, High Performance Hardware Implementation for RC4 Stream Cipher, DOI 10.1109/TC.2012.19 2012 *IEEE Transactions on Computers.*

[8] Boland, H. Mousavi, Security issues of the IEEE 802.11b wireless LAN, *Canadian Conference of Electrical and Computer Engineering (CCECE)*, 2004.

[9] X. Zhang and K. K, Parhi, High-speed VLSI Architecture for the AES Algorithm, *IEEE Trans. on VLSI Systems, vol.12(9), pp. 957-967, Sep. 2004.*

[10] N Sklavos, G Selimis and O Koufopavlou, FPGA implementation cost and performance evaluation of IEEE 802.11 protocol encryption security schemes, *Journal of Physics: Conference Series* ***10*** *(2005) 361–364.*

[11] Vinay Bhatia, Dushyant Gupta and H.P. Sinha Throughput and Vulnerability Analysis of an IEEE 802.11b Wireless LAN, *International Journal of Computer Applications (0975 – 8887) Volume 52– No.3, August 2012*

[12] Sumanth Kumar Reddy S, R Sakthivel, P.Praneeth "VLSI Implementation of AES Crypto Processor for Higher Throughput" *International Journal of Advanced Engineering Science and Technologies* Vol-6, Issue.No.1, Pg:22-26, May 2011.

[13] M Vanitha, R Sakthivel and Subha "Highly Secured High Throughput VLSI Architecture for AES Algorithm" in proceedings of *International Conference on Devices, Circuits and Systems* – ICDCS 2012.