Performance Comparison of EAP-GPSK, SAKE with AES-CCM and EAP-SAKE-FFX Authenticated Encryption Protocols for WiMAX Network Security

B. Chandran Mahesh[1], **Dr. B. Prabhakara Rao**[2]

[1]Nimra College of Engineering & Technology, Assistant Professor, Department of ECE, Ibrahimpatnam

[2]JNT University, Kakinada, Former Rector, Department of ECE

Abstract: ***WiMAX technology is a broadband wireless data communications technology based around the IEEE 802.16 standards providing high speed data over a wide area. Developed nations desire to install a new high speed data network very cheaply to those in rural areas needing fast access where wired solutions may not be viable because of the distances and costs involved. WiMAX Network security is a measure to protect the data during the transmission between client and server. Security attack is an action that compromises the security of information over the network by the third party. The security mechanisms are designed to detect, prevent and recover the information from a security attack. Authentication is the process of verifying the identity of a authorized user or a device to access the network resources and information. There is an increasing demand to provide strong authentication for users, devices and applications across all types of network. The level of security offered by passwords is very low [1]. The level of security could be increased by using two or three factor authentication. Authentication Protocol uses message formats to communicate between client and server. It supports authentication mechanisms such as smartcards, Kerberos, digital certificates, onetime passwords and others. The authentication protocol is extensible when any one of the above authentication mechanisms is encapsulated within the message formats. Secure user authentication is obtained through the encrypted exchange of the user's credentials. Authentication mechanisms are implemented in a number of ways called EAP methods such as EAP-TLS, EAP-TTLS, EAP-PEAP etc. We compare and analyze the performance of existed authenticated protocols EAP-GPSK, EAP-SAKE with AES-CCM encryption algorithm and the proposed hybrid protocol EAP-SAKE with AES-FFX, format preserving encryption algorithm to provide security to the base stations of WiMAX network.***

Keywords: Channel Binding, Key Derivation Function, Format-preserving encryption, message integrity check.

1. Introduction

WiMAX, short for Worldwide Interoperability for Microwave Access, is the name for 802.16e standard of wireless network services. WiMAX is aimed at carriers for use in metropolitan area networks. It has a tremendous range, up to 30 miles, and a speed of up to 100 Mbps. WiMAX has important flavours of 802.16 standards with different capabilities [2].

In Wimax applications only encryption is not enough to provide the utmost level of security. Eighty percent of the Wimax applications use an open source operating systems. Open source allows third parties to change the original code according to their own requirements and needs. So it is not sufficient to use only encryption techniques to protect the information but authenticated encryption Techniques are required.

Significant amount of research and effort has been involved to invent more proficient authenticated encryption algorithms. This paper talks of comparison of extensible authenticated protocols EAP-GPSK, EAP-SAKE with AES-CCM encryption and EAP-SAKE with hybrid encryption scheme AES-FFX.
This paper is organized into the following sections: Section-2 explains the description of EAP-GPSK and EAP-SAKE authenticated protocols. Section-3 discusses the AES-CCM and AES-FFX encryption algorithms. Section-4 shows the performance analysis of three EAP methods. Section-5 proposes the conclusion.

2. Description of Extensible Authenticated Protocol (EAP) methods

EAP is an access authentication framework that was originally developed to support peer authentication before granting the peer access to the network [3]. The actual cryptographic schemes used for achieving the desirable security objectives are defined in the EAP methods. With the growing complexity of applications and security demands, the scope of the security objectives and features has been extended to include server authentication, key establishment, privacy and many other features. This section describes the EAP-GPSK and EAP-SAKE message sequence charts.

2.1. EAP-GPSK

EAP Generalized Pre-shared key (GPSK) method [4][5] is a lightweight shared-key authentication protocol that supports mutual authentication of the user and the server and the key derivation. Lightweight refers to more sure than previous protocols and easy to implement. EAP-GPSK exhibits low computational overheads as it does not make use of any public key cryptography, but instead fully relies on symmetric cryptography.

The following fields are present in the respective GPSK framework messages shown in Figure 1.

- Message 1: EAP-GPSK Header, ID_Server, RAND_Server and CSuite_List.
- Message 2: EAP-GPSK Header, ID_Client, ID_Server, RAND_Client, RAND_Server, Csuite_List, Csuite_Sel and the MAC.
- Message 3:EAP-GPSK Header, RAND_Client, RAND_Server, CSuite_Sel and the MAC.
- Message 4: EAP-GPSK Header and the MAC The ID_Client and ID_Server.

Fields used in the GPSK messages are each 100 Bytes as they carry the identities of the server and the client respectively. The CSuite_List is a list possible cipher suites (6 Bytes each) that may be used.

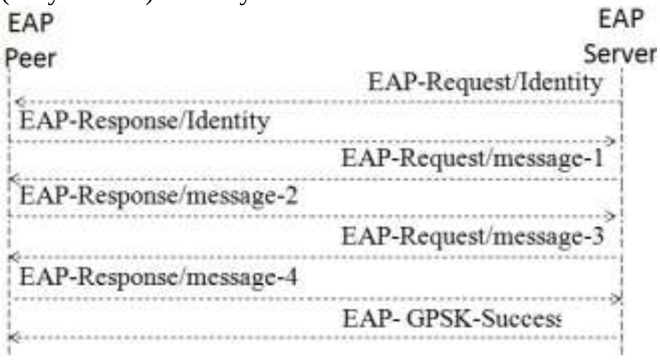


Figure 1: EAP-GPSK Successful l Exchange Process

It is assumed that 10 such cipher suites are carried in the message, and hence the size of the complete CSuite_List is 60 Bytes. It is also assumed that no optional payload is present and the cipher suite 2 (i.e. HMAC-SHA256) is used for generation of the Message Authentication Code [6].

2.2 EAP-SAKE

EAP Shared-secret Authentication and Key Establishment (SAKE) [7] method supports mutual authentication of the client and the server and session key derivation based on a static pre-shared secret data. EAP-SAKE is based on the Bellare-Rogaway mutual authentication mechanism. The following fields are present in the respective SAKE messages shown in Figure 2 framework.

• Challenge 1: EAP-SAKE Header, RAND_S and Server_ID.
•Challenge 2: EAP-SAKE Header, RAND_P, Peer_ID, SPI_P and MIC_P.
•Confirm 1: EAP-SAKE Header, SPI_S, ENCR_DATA, MIC_S.
• Confirm 2: EAP-SAKE Header and MIC_P.

The peer Network Access Identifier (NAI) used in the EAP-SAKE messages is assumed to be 100 Bytes. The Security Parameter Index (SPI) is assumed to be compatible with IPSec and hence is 4 Bytes in size. The optional Initialization Vector attribute and the optional encrypted data field are not used.

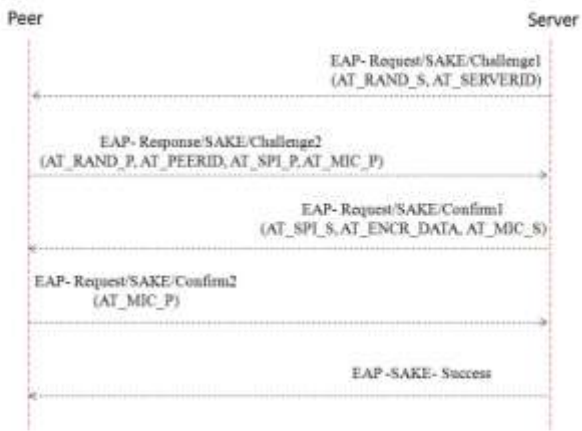

Peer
Server
EAP- Request/SAKE/Challenge1
(AT_RAND_S, AT_SERVERID)
EAP- Response/SAKE/Challenge2
(AT_RAND_P, AT_PEERID, AT_SPI_P, AT_MIC_P)
EAP- Request/SAKE/Confirm1
(AT_SPI_S, AT_ENCR_DATA, AT_MIC_S)
EAP- Request/SAKE/Confirm2
(AT_MIC_P)
EAP -SAKE- Success

Figure 2: EAP-SAKE Authentication procedure

3. Description of AES Encryption Schemes

3.1 Traditional AES-CCM mode Encryption

Advanced Encryption Standard, or AES, [8] is the standard known for a symmetric block cipher mechanism that uses 128 bits, 192 bits and 256 bits of key sizes. CCM is an Authenticated Encryption Standard which is based on a key management structure. In this algorithm, the plaintext is divided into block ciphers of 128 bits size. The modes of operations used in AES-CCM are counter mode (CTR) with Cipher Block Chaining and Message Authentication Code (CBC-MAC). They perform generation-encryption and decryption-verification functions [8]. The confidentiality feature is achieved in CTR mode by AES and the authentication is achieved in CBC-MAC with the MAC value generated as shown in figure 3.

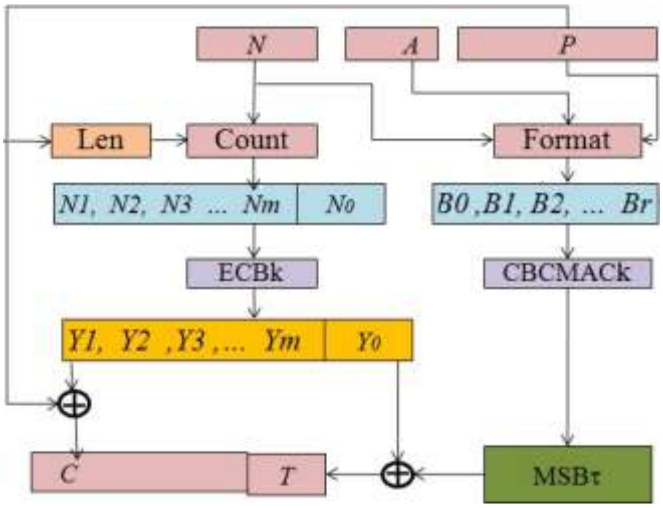
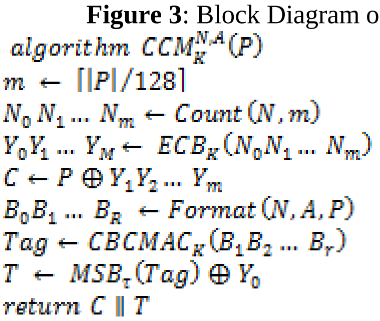


Figure 3: Block Diagram of CCM Encryption



```
algorithm $CCM_K^{N,A}(P)$
$m \leftarrow \lceil |P|/128 \rceil$
$N_0 N_1 \ldots N_m \leftarrow Count(N, m)$
$Y_0 Y_1 \ldots Y_M \leftarrow ECB_K(N_0 N_1 \ldots N_m)$
$C \leftarrow P \oplus Y_1 Y_2 \ldots Y_m$
$B_0 B_1 \ldots B_R \leftarrow Format(N, A, P)$
$Tag \leftarrow CBCMAC_K(B_1 B_2 \ldots B_r)$
$T \leftarrow MSB_\tau(Tag) \oplus Y_0$
return $C \parallel T$
```

The process of decryption of an AES cipher text is similar to the encryption process in the reverse order.

3.2 Proposed AES-FFX Scheme to Encapsulate in EAP-SAKE Authentication Protocol

The approved modes prevail for encryptions are transformations on binary data, i.e., the input and output of the modes are bit strings—sequences of ones and zeros. Format-preserving encryption (FPE)[9] is designed for data that is not necessarily binary. In particular, given any finite set of symbols, like the decimal numerals, a method for FPE transforms data that is formatted as a sequence of the symbols in such a way that the encrypted form of the data has the same format, including the length, as the original data. Thus, an FPE-encrypted Social Security number would be a sequence of nine decimal digits.

FPE facilitates the targeting of encryption to sensitive information, as well as the retrofitting of encryption technology to legacy applications, where a conventional encryption mode might not be feasible. For example, database applications may not support changes to the length or format of data fields. FPE has emerged as a useful cryptographic tool, whose applications include financial-information security, data sanitization, and the transparent encryption of fields in legacy databases.

The two FPE modes specified in this publication are abbreviated FF1 and FF3, to indicate that they are format-preserving, Feistel-based encryption modes.FFX schemes, including FF1 and FF3, are based on the Feistel structure. The Feistel structure consists of several iterations, called rounds, of a reversible transformation.

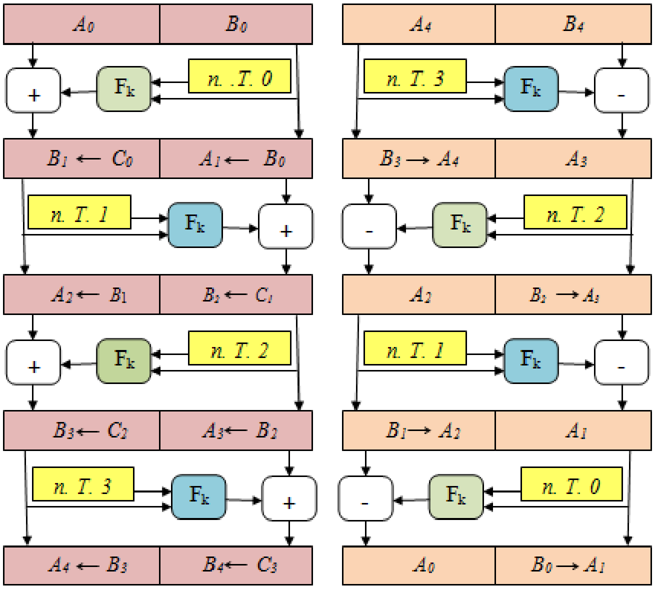


Figure 4: Feistel Structure for FFX scheme

The transformation consists of three steps: 1) the data is split into two parts; 2) a keyed function, called the round function, is applied to one part of the data in order to modify the other part of the data; and 3) the roles of the two parts are swapped for the next round. The structure is illustrated in Figure 4 below, for both encryption and decryption. Four rounds are shown in Figure 4, but ten rounds are actually specified for FF1 and eight rounds for FF3 [9].

For the encryption function in Figure 4, the rounds are indexed from 0 to 3. The input data and output data for each round are two strings of characters—which will be numerals for FFX. The lengths of the two strings are denoted by u and v, and the total number of characters is denoted by n, so that u+v = n. During Round i, the round function, denoted by F_K, is applied to one of the input strings, denoted by Bi, with the length n, the tweak T, and the round number i as additional inputs. In Figure 4, this triple (n, T, i) of additional inputs is indicated within the dotted rectangles, with the appropriate values for i. The result is used to modify the other string, denoted by Ai, via modular addition4, indicated by +, on the numbers that the strings represent5. The string that represents the resulting number is named with a temporary variable, Ci. The names of the two parts are swapped for the next round, so that the modified Ai, i.e., Ci, becomes B_{i+1}, and Bi becomes A $_{i+1}$.

The rectangles containing the two parts of the data have different sizes in order to illustrate that, u cannot equal v if n is odd. In such cases, the round function is constructed so that the lengths of its input and output strings depend on whether the round number index, i, is even or odd.

The Feistel structure for decryption is almost identical to the Feistel structure for encryption. There are three differences: 1) the order of the round indices is reversed 2) the roles of the two parts of the data in the round function are swapped as follows: along with n, T, and i, the input to F_K is A_{i+1} (not Bi), and the output is combined with Bi_{+1} (not Ai) to produce Ai (not B_{i+1}) and 3) modular addition (of the output of F_K to Ai) is replaced by modular subtraction (of the output of F_K from $B_{i +1}$).

4. Performance Evaluation

A WiMAX network [9] simulation model is designed with the following specifications as mentioned in Table 1.

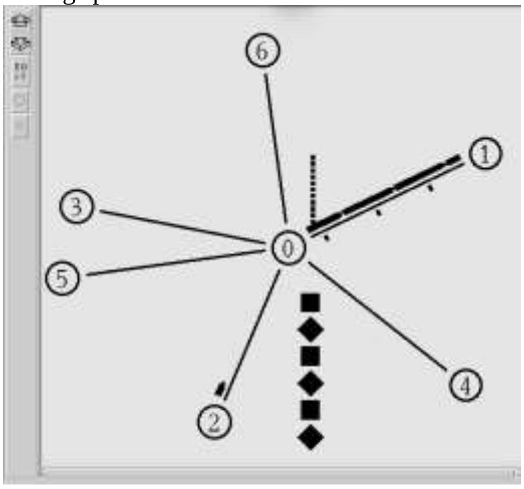


Figure 5: WiMAX Simulation Model with Attackers

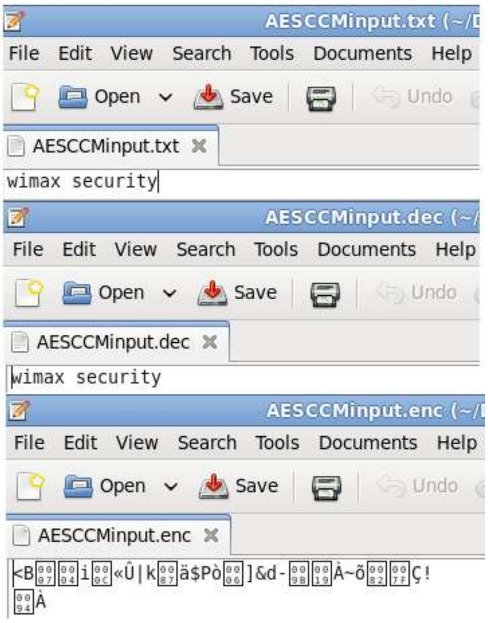
The EAP mechanisms are implemented in the WiMAX simulation model [10]. Throughput is the number of successfully received packets in a unit time and it is represented in Mbps. Throughput and Drop rate is calculated from the trace file generated after execution of simulation process for a transmission period of 800ms. Performance metrics Avg.throughput and drop rate are calculated by varying no. of Attackers as mentioned in the table-1.

Table 1: Simulation Parameters of WiMAX network

Parameter	*Specifications*
Area Size	1100 X 1100
MAC	802.16
No. of Mobile Nodes	5,10,15,20 and 25
Radio Range	250m
Simulation Time	50 sec
Physical Layer	OFDM
Packet Size	500 bytes
Frame Duration	0.005
Rate	1Mb
No. of Attackers	2,4,6,8 and 10

4.1. Encipherment of AES Schemes

Encipherment provides data confidentiality services by transforming data into not-readable forms for the unauthorized persons. This mechanism uses encryption-decryption algorithm with secret keys. AES-CCM encryption is verified by giving text as input to encryption process and getting the same text after decryption as shown in Figure 6.



AESCCMinput.txt (~/D

AESCCMinput.txt

wimax security

AESCCMinput.dec (~/

AESCCMinput.dec

wimax security

AESCCMinput.enc (~/

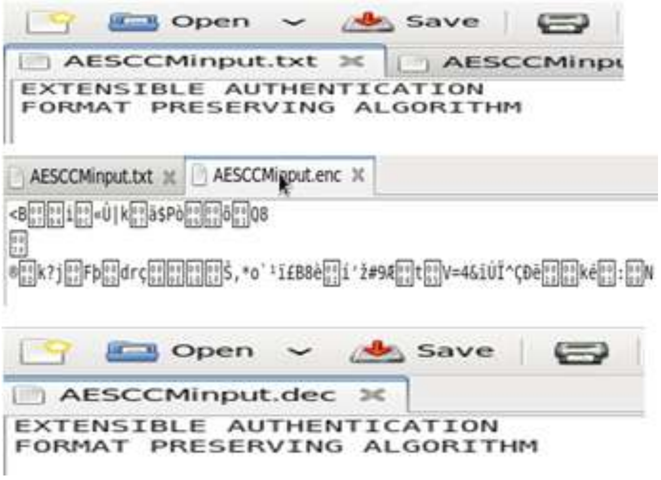
AESCCMinput.enc

<B□□i□«Û|k□ä$Pò□]&d-□□À~õ□□Ç!
□À

Figure 6: Verification of AES-CCM Scheme

4.2. Encipherment of AES-FFX schemes

Encipherment of AES-FFX scheme is verified by giving text as input to encryption process and getting the same text after decryption as shown in Figure 7.



AESCCMinput.txt

AESCCMinpu

EXTENSIBLE AUTHENTICATION
FORMAT PRESERVING ALGORITHM

AESCCMinput.txt

AESCCMinput.enc

<B□□i□«Û|k□ã$Pò□□ö□08
□
®□k?j□Fþ□drç□□□□Š,*o'¹ï£B8è□í'ž#9Æ□t□V=4&ïÙÏ^ÇĐë□□kë□:□N

AESCCMinput.dec

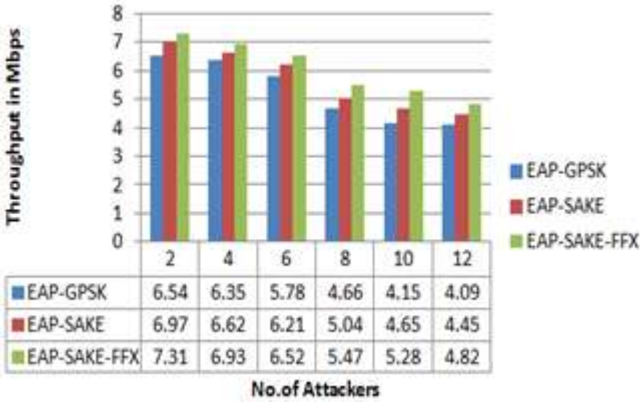
EXTENSIBLE AUTHENTICATION
FORMAT PRESERVING ALGORITHM

Figure 7: Verification of AES-FFX Scheme

4.3. Performance Comparison of EAP methods

AES-CCM encryption is encapsulated in message formats of EAP-GPSK and EAP-SAKE protocols and .AES-FFX scheme is encapsulated in EAP-SAKE and performance metrics of three protocols are calculated.

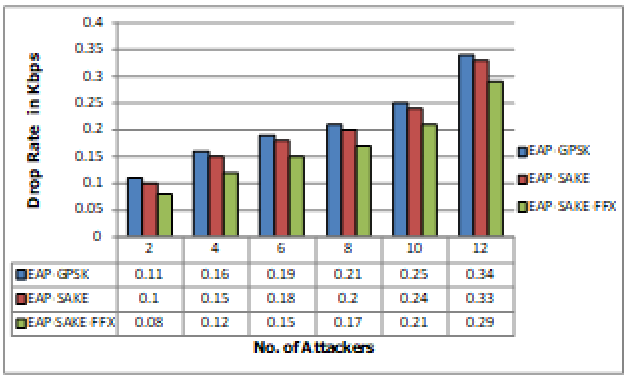
Throughput is calculated in Mbps by varying attackers as 2, 4, 6, 8 and 10 in the network in each EAP protocol. It is observed that throughput of EAP-SAKE-FFX is 15.07 % greater than EAP-GPSK as shown in Figure 7.



	2	4	6	8	10	12
EAP-GPSK	6.54	6.35	5.78	4.66	4.15	4.09
EAP-SAKE	6.97	6.62	6.21	5.04	4.65	4.45
EAP-SAKE-FFX	7.31	6.93	6.52	5.47	5.28	4.82

Figure 7: Comparison of Avg. Throughput – EAP methods

Drop Rate is calculated in kbps by varying attackers as 2, 4, 6, 8 and 10 in the network in each EAP protocol. It is observed that Drop Rate of EAP-SAKE-FFX is 19.04% lesser than EAP-GPSK as shown in Figure 8.



	2	4	6	8	10	12
EAP GPSK	0.11	0.16	0.19	0.21	0.25	0.34
EAP SAKE	0.1	0.15	0.18	0.2	0.24	0.33
EAP SAKE FFX	0.08	0.12	0.15	0.17	0.21	0.29

Figure 8: Comparison of Avg. Drop rate - EAP Methods

5. Conclusion

The recent version of WiMAX, IEEE 802.16e for mobile applications fixed and rectified many of the problems highlighted in 802.16d by adding data integrity mechanisms, mutual authentication, and AES-CCM for data packet encryption. The security level of proposed scheme EAP-SAKE-FFX is improved comparatively than existing protocols to protect the services of WiMAX base stations against unauthorized Base station Attacks and Distributed denial of service Attacks.

6. Future Scope

The security offered by FF1 and FF3 may be affected by the values of the parameters, e.g., radix, minlen, and maxlen. Encrypted data may be vulnerable to guessing attacks when the number of possible inputs is sufficiently small. The third mode FF2 did not provide expected 128 bits security strength. The extension of the FF2 proposal submitted to NIST for consideration [11].

References

[1] A. K. Rai, V. Kumar, and S. Mishra, “An efficient password authenticated key exchange protocol for WLAN and WiMAX,” in Proceedings of the International Conference & Workshop on Emerging Trends in Technology, pp. 881–885, ACM, February 2011.

[2] Lukasz Kucharzewski and Zbigniew Kotulski: “WiMAX Networks-Architecture and data security”2010, Annales UMCS Informatica (AIX).

[3] L. Blunk, 1. Vollbrecht, “Extensible Authentication Protocol (EAP)”,Request for Comments 3748, June 2004.

[4] F. Bersani and H. Tschofenig, “The EAP-PSK Protocol: A Pre-Shared Key Extensible Authentication Protocol (EAP) Method”, IETF RFC 4764, January 2007.

[5] T. C. Clancy and H. Tschofenig, “EAP Generalised Pre-Shared Key (EAP-GPSK)”, draft-ietf-emu-eap-gpsk-02.txt, work in progress, January 2009.

[6] NIST Special Publication (SP) 800-107, Recommendation for Applications Using Approved Hash Algorithms, (Revised), (Draft) September 2011.

[7] M. Vanderveen and H. Soliman, “Extensible Authentication Protocol method for Shared secret Authentication and Key Establishment (EAP-SAKE)”, IETF RFC 4763 November 2006.

[8] National Institute of Standards and Technology Special Publication 800-38C Natl. Inst. Stand. Technol. Spec. Publ. 800-38C28 pages (March 2016).

[9] M. Bellare, P. Rogaway, and T. Spies, “The FFX Mode of Operation for Format-Preserving Encryption” (2/18/2016).

[10] Network Simulator: http:///www.isi.edu/nsnam/ns.

[11] M. Dworkin and R. Perlner, Analysis of VAES3 (FF2), Report no. 2015/306, IACR Cryptology ePrint Archive, April 2, 2015, http://eprint.iacr.org/2015/306.[accessed 2/18/2016].

Author Profile

Dr. Bhima Prabhakara Rao graduated in the discipline of ECE, from SV University, Thirupathi with B.Tech M.Tech Degrees in the years 1979&1981, received his doctoral degree from Indian Institute of Science, Bangalore in the year 1995. He is having of 34 years Teaching Experience as director of Evaluation, Rector and ViceChancellor.19-doctoral degrees were awarded with 252 research papers in international and national journals. He is recipient of AP State Govt. Best Teacher awardee for the year 2010.He served Honorary Chairman for Institution of Engineers, for IETE Sub center Kakinada 2011-2016.He was elected as Fellow of Engineers, Fellow of IETE, Senior IEEE member.

Chandran Mahesh Bondalapati received his B.Tech. and M.Tech., degrees in Electronics and communications Engineering from Nagarjuna university and JNTU, Anantapur in 1998 and 2007, respectively. During 1998-2001, he had been working as communication engineer in the field of commissioning of satellite signals through VSAT antennas. Now he is working as Assoc. Professor in Dept.of ECE and pursuing his Ph.D. in JNTUK, Kakinada. Inspiring Teacher Awardee in Regency Institute of Tech., yanam in 2009.