SECURED BROADBAND DATA ACCESS SYSTEM IN WIMAX

Ancy Anna Mani*

Dr. V.Gopi**

Abstract—

Security mechanism is to meet the expectations from mobile users to provide seamless services in mobile WiMAX. Handover should take place in highly secured and in most improved means. The main motive of the mobile technologies is to provide seamless cost effective mobility. But this is affected by Authentication cost and handover delay since on each handoff the Mobile Station (MS) has to undergo all steps of authentication. To overcome these vulnerability we propose an Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers (HO) using WPKI (wireless public key infrastructure). In this approach, a improved X.509 certificate is generated based on Elliptical Curve Cryptography (ECC) algorithm, then an enhanced mutual authentication flow, which enhances the security and working efficiency of the mutual authentication in multi-hop WiMax system is designed. Asymmetric key cryptography is used to secure the pre-authentication message exchange with low demand of computational resource. The proposed scheme can also meet the security requirements of an authentication protocol. The proposed scheme increases the security and practicability of WiMax system, which has better referenced value to the improvement of IEEE 802.16e standards. The proposed work is simulated by NS2 model and by MATLAB

Keywords—Elliptical Curve Cryptography, Handover, Security, WiMAX, Wireless Public Key Infrastructure.

* PG Student, M.E (CS), PSN College of Engineering and Technology,Tirunelveli.

** Professor, M.E (CS), PSN College of Engineering and Technology, Tirunelveli.

I. INTRODUCTION

WiMAX is neoteric technology providing broadband data access to mobile and stationary users while supporting handover and roaming capabilities. It is a technology based on IEEE 802.16 standards[1].The security sub layer of IEEE 802.16d[1] standard defines the security mechanism for fixed and IEEE 802.16e[2] standard defines the security mechanism for mobile networks. The security sub layer supports are to: (i) authenticate the user when the user enters in to the network (ii) authorize the user, if the user is provisionised by the network service provider, and then (iii) provide the necessary encryption support for the key transfer and data traffic. Since 2005 Mobility support has been included into the IEEE 802.16e standard.

Mobile WiMAX system supports handover processes to make a mobile station (MS) find another base station (BS) from the same or different access service network (ASN) to establish connection when moving out of coverage of the current serving BS (home BS or hBS). The MS and the target BS (tBS) or target ASN gateway, or ASN-GW (tASN) have to authenticate each other before the MS is granted access to the network to meet the security requirements. Extensible Authentication Protocol (EAP)-based authentication [3] is one of the authentication mechanism supported by the IEEE 802.16e. EAP based authentication uses a backend authentication server (AS) such as an authentication, authorization, and accounting (AAA) server, which allows users to choose an authentication method suitable for the existing credentials without requiring the authenticator to be updated to support each new authentication approach. The flexibility makes the EAP-based authentication a popular authentication method for mobile WiMAX systems.

The MS will perform a full EAP authentication with the AS and perform a Security Association's traffic encryption key (SATEK) when a MS handovers from one BS to another in different ASNs, this is referred as an inter-ASN handover, 3-way handshake with the BS to distribute the TEK. The handover process should be fast to maintain seamless service connections. However, an EAP-based authentication has been well known to be costly due to its time-consuming public key cryptography operations and the delay of several round-trips between the MS and the AS. A full EAP authentication takes about 1000ms, while the recommended maximum handover latency for streaming applications is only 150 ms [4].

To reduce the handover latency, mobile WiMAX supports handover optimization, allowing users to reduce handover latency by reusing key materials from previous authentication [5]. However, it creates critical security holes such as a lack of valid entity authentication leading to Man in-the-Middle (MITM) attacks. Alternative solutions have focused on reducing the delay incurred in the EAP authentication, which is the majority of the handover latency, without compromising security requirements. The current techniques mainly fall into two categories, namely the re-authentication and the pre-authentication.

Re-authentication can avoid full EAP-based authentication in handover by reusing the information exchanged between the MS and the AS in the previous authentication. In [5], the HOKEY working group has proposed the EAP re-authentication protocol (ERP) which allows a MS and the AS to use the extended master session key (EMSK) authentication for master. Re-authentication techniques can lower the authentication signalling latency.

By pre-authentication techniques in [6]–[8], a MS and the AS pre-compute the shared secret keys before. Thus, the handover delay could be effectively reduced to the same amount of the time used by a 3-way handshake, resulting in the shortest authentication signalling delay. The main advantage of the pre-authentication is that the cryptographic material will not be reused, hence it becomes more secure. The HOKEY working group has proposed an EAP based pre-authentication model in [6] which has been adopted to Mobile IPv6 network in [7] and is called Handover Early Authentication (HOEA) protocol. An EAP-based pre-authentication scheme (EPA) reduce the authentication delay in inter-ASN handovers [9] .We propose an Enhanced EAP-based, or specifically, the EAP-Transport Layer Security (EAP-TLS) based pre-authentication (EEP) scheme for fast and secure inter-ASN handovers (HO) using WPKI (wireless public key infrastructure)which can prevent DoS and replay attacks with much less computational and communication resources and at the same time.

The rest of the paper is organized as followed. The network model and the EAP-TLS based authentication are described in Section 2. Our proposal are presented in Section 3. And finally, in Section 4, we conclude the paper with a summary.

II.SYSTEM BACKGROUND

A. Network Model

Mobile WiMAX network reference model (NRM), the system under the study consists of three logical parts: a MS, an ASN owned by a network access provider (NAP), and a connectivity service network (CSN) owned by network service provider (NSP). An ASN is formed by BSs and an ASN-GW to offer radio access to MSs. An ASN-GW is placed at the boundary of the ASN and connects the BSs to the CSN, which provides IP connectivity service to the MSs. The authenticator is located at the ASN-GW. The AS, which supports the authentication for the MSs, resides in the CSN. There are two types of handovers in the specified mobile WiMAX systems. One type is the intra-ASN handover, which happens when a MS moves between BSs in the same ASN. Another one is the inter-ASN handover, which happens when a MS moves from a BS in one ASN to another BS in a different ASN.

B. The EAP Framework and Authentication

Since the EAP-TLS based authentication provide strong mutual authentication [8], it has been selected by the WiMAX forum as one of the options for the specification of the authentication procedure between the MS and the AS. The EAP authentication is executed between a MS and the BS in the Privacy Key Management version 2 security protocol [9]

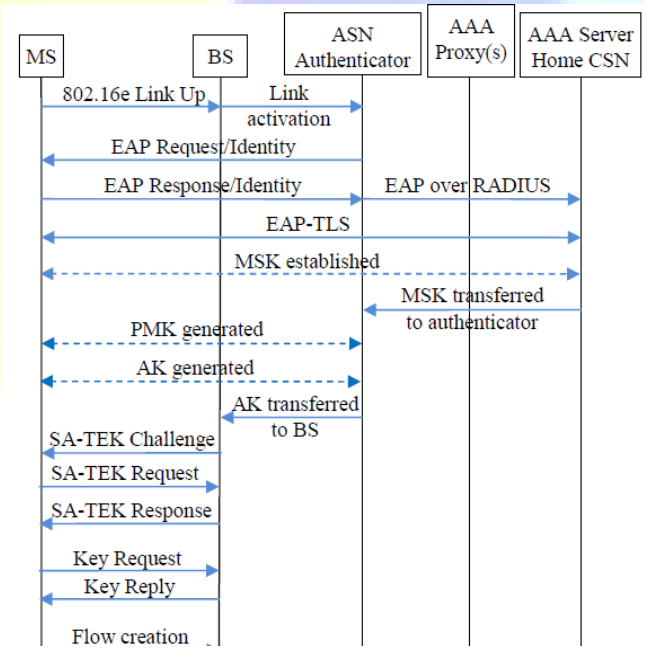

Fig. 1. EAP-TLS-based authentication.

specified by the IEEE 802.16e standard. Procedure of EAP-TLS-based authentication [10] is shown in Fig.1.

First of all, the MS issues a link-up request message to the BS. The BS then relays an EAP message to the authenticator in the ASN. From there, the EAP message is carried to the AS over RADIUS [11]. After the authentication process, the MS and the AS generate a MSK, which will be transferred to the authenticator in the ASN. The MSK is used for both the authenticator and the MS to generate a pair-wise master key (PMK) and an AK. The AK is transferred to the hBS, which is used for the SA-TEK 3-way handshake and key exchange. At the end of the authentication, both the MS and the BS share the TEK for the data encryption.

III. PROPOSED SCHEME

The Existing Approach is a insecure EAP-based pre-authentication scheme for the inter-ASN HOs. To face the challenges in the design of efficient and robust authentication protocols for HOs, asymmetric key cryptography is used to secure the pre-authentication message exchange with low demand of computational resource. An improved X.509 certificate based on ECC algorithm is designed, then an enhanced mutual authentication flow was proposed in this project, which enhances the security and working efficiency of the mutual authentication in multi-hop WiMax system. It can overcome the abovementioned drawbacks by allowing the MS to exchange the secret keys with the AS instead of the neighbour ASNs (nASNs).In this section, we present the proposed EEP scheme for inter-ASN handovers, which fully utilizes the following information provided from the previous EAP-TLS mutual authentication and the centralized AS to prevent the attacks and reduce the number of cryptographic operations required.

A Public Key Infrastructure (PKI) is a system consisting of set of hardware and software used for the management of public key and distribution of digital certificates which are used to verify a particular public key belongs to a certain entity. The PKI creates digital certificates which map public keys to entities, securely stores these certificates in a central repository, and revokes them if needed when it is not in use. Public key cryptography is used to transmit user's public key in PKI environment. Public key of the user is advertised and corresponding private key kept secret. A PKI consists of Certification Authorities (CAs), Registration Authorities (RAs), Certificate holders, Clients, Repositories, Cryptographic [13-18] Algorithms and Protocols. A Public Key Infrastructure ensures the following:

- Ensures the quality of information transmitted over the network.
- Lifetime and validity of the information.
- Certainty of the privacy, and source and destination of that information of that information.
- To ensure non repudiation.

The principal attraction of Elliptic Curve Digital Signature Algorithm is that, it offers equal security for a small key size as that of RSA, thereby reducing processing overhead. ECC based Elliptic Curve Digital Signature Algorithm generates 163-bit key size, equivalent to RSA 1024-bit key size, it takes shorter time to generate public key pair in mobile phone than RSA algorithm. Since ECDSA 163-bit key size is less than RSA 1024-bit key size, a certificate size including the public key could be reduced .

Then Enhanced mutual authentication flow was proposed in this project, which enhances the security and working efficiency of the mutual authentication in multi-hop WiMax system. It can overcome the drawbacks by allowing the MS to exchange the secret keys with the AS instead of the neighbour ASNs (nASNs)In this section, we present the proposed EEP scheme for inter-ASN handovers, which fully utilizes the following information provided from the previous EAP-TLS mutual authentication and the centralized AS to prevent the attacks and reduce the number of cryptographic operations required. Various steps taking place in EEP are:

Firstly, it is assumed that the hBS always has an updated AS's certificate. This certificate can be obtained indirectly when the hBS relays the certification exchange during the EAP-TLS hand-shaking between the AS and the MS [12] or it can periodically request and check validation status of the AS's certificate.

Secondly, after the mutual authentication, the MS and the hBS share the message authentication code (*MAC*) key, which is used to calculate Hash-based or cipher-based *MAC* of management messages in order to facilitate the message authentication and integrity.

Lastly, the ASN authenticator can communicate with the AS securely using the RADIUS protocol.

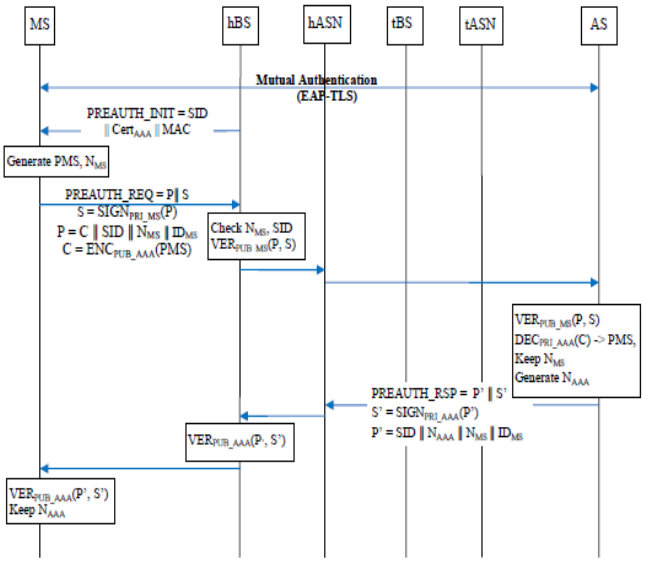

Fig. 2. The EEP pre-authentication scheme.

The ASN authenticator and the AS share a secret key that can be used to protect data confidentiality.

TABLE I

BASIC DEFINITION

PUK A	Public key of A
ENCK(X)	Encrypt X using K
PRK A	Private key of A
DECK(X)	Decrypt X using K
SIGNK(X)	Generate Signature for message X using K
V ERK(X, S)	Verify message X with the corresponding signature S using K
IDA	Identifier of A
TLS-PRF-X TLS	pseudo-random function computed to *X* octets

The AS can be employed to securely distribute the *MSK* to the nASN after it is confirmed to be the tASN for a handover. With the above facts, by the EEP scheme, the MS has only to exchange a pre-master secret (*PMS*) with the AS, which will use this *PMS* together with other available information to generate the corresponding *MSK* and send it over the RADIUS to the tASN.

Various steps included are:

- 0*th* Step: After the MS finishes the mutual authentic ation with the AS, the AS and the hBS are trusted by the MS. The hBS shares the *MAC* key with the MS.
- 1*st* Step: The hBS sends a *PREAUTH INIT* containing a unique 16-bit session identifier (*SID*), the updated and verified AS's certificate and the *MAC* to the MS. The *SID* is incremented whenever the hBS initiates a new pre-authentication session with the same MS.
- 2*nd* Step: The MS checks the *SID* and the *MAC* to make sure that it is not a replayed message and is from the hBS. After that, it randomly generates a *PMS* and a nonce *NMS*. The *PMS* is encrypted using the AS's public key. It is concatenated with the *SID*, newly generated nonce and the *IDMS*. After that, the message is signed using the MS's private key and sent to the hBS. The hBS verifies the signature using the MS's public key to check whether the message has been modified. It also checks the *SID* and the *NMS* to make sure it is the reply of the *PREAUTH INIT* sent previously and it is not a replayed message. After that, it relays the message to the AS.
- 3*rd* Step: The AS verifies the signature of the received message and the *NMS* to make sure it has not received this message before and the message has not been tampered. If the message is genuine, the AS will decrypt the cipher text using its private key to obtain the *PMS*. It will then generate a nonce *NAAA*, concatenate it with the *SID*, the *NMS* and the *IDMS*, sign the message and send it back to the hBS. Similar to the step 2, the hBS will verify the message and relay it to the MS. The MS can verify the correctness of the receiving message and keep a record of the *NAAA*.

The handover phase (Fig. 3) begins with a decision for an MS to handover from the hBS to a tBS. The decision may originate either at the MS or the hBS using *MOB MSHOREQ* or *MOB BSHO-REQ* message, respectively. Before the handover decision is made, the hBS sends a notification containing the *IDMS*, *IDtASN* and the Carrier to Interference plus Noise Ratio (*CINR*) to the possible tBS over the backbone to notify the tBS of the MS intent for handover [13]. If the tBS

accepts to handover, it will send a handover notification response through the backbone to the hBS. The message will go through the tASN. As it is informed that it is selected for the handover, the tASN will send a *KEY REQ* to the AS containing the *IDMS* and *IDtASN* to the AS.

After above steps, the MS and the tASN share the same *MSK*, compute the *AK* and continue with the SA-TEK 3-way handshake as specified by IEEE 802.16e standard. The EEP inherits EPA's ability to prevent eavesdropping, impersonation and MITM attacks. Firstly, the *PMS* is encypted by using public key of the AS, preventing an adversary from eavesdropping the secret.

Secondly, it is impossible for an adversary to impersonate one honest party to send message to another party because each message is either signed using the transmitter's private key or protected by the *MAC*. A MITM attack is also impossible because the pre-authentication process is a mutual authentication, which implies that all communication parties are required to provide a proof of the identity by using a certificate, a digital signature or a *MAC*.

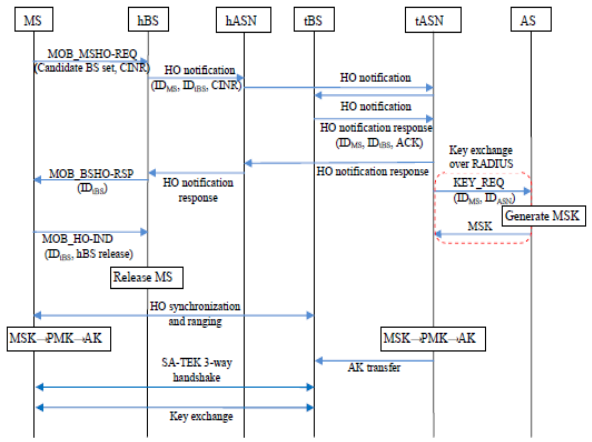

Fig. 3. The handover when EEP is used.

The adversary cannot register itself as a legitimate MS or an ASN as long as it does not have the *MAC* key or the private key of the communication party whom it wants to impersonate.

A. Advantage of ECC over RSA

The main advantage ECC has over RSA is that the basic operation in ECC is point addition, which is known to be computationally very expensive. This is one of the reasons why it is very unlikely that a general sub-exponential attack on ECC will be discovered in the near future, though ECC has a few attacks on a few particular classes of curves. These curves can be readily distin-

guished and can be avoided. On the other hand, RSA already has a known sub-exponential attack which works in general. Thus, to maintain the same degree of security, in view of rising computing power, the number of bits required in the RSA generated key pair will rise much faster than in the ECC generated key pair, as seen in table 2. Using smaller key, we require low computational time, low computational power & small memory. As it requires low computational power, the battery life will get increases.

Table 2: Comparison of strength of RSA and ECC

Time to break RSA key-size ECC key-size (in MIPS-years)	RSA key-size In bits	ECC key-size In bits
104	512	106
108	768	132
1011	1024	160
1020	2048	210
1078	21000	600

IV. RESULT

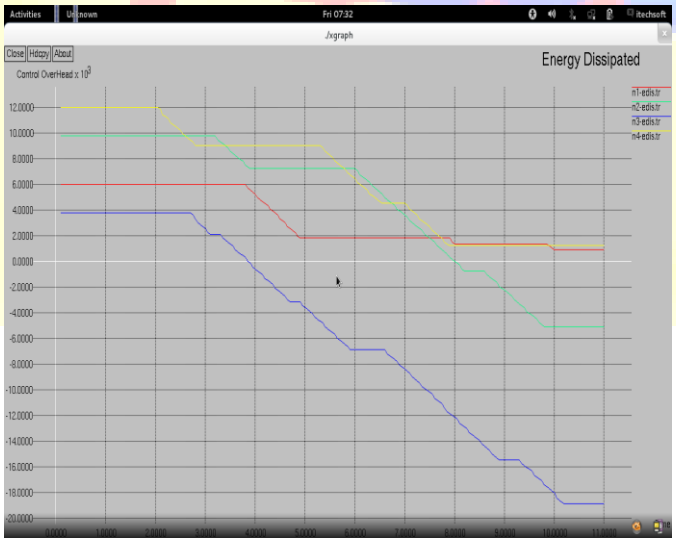

Fig.4. Energy Dissipated

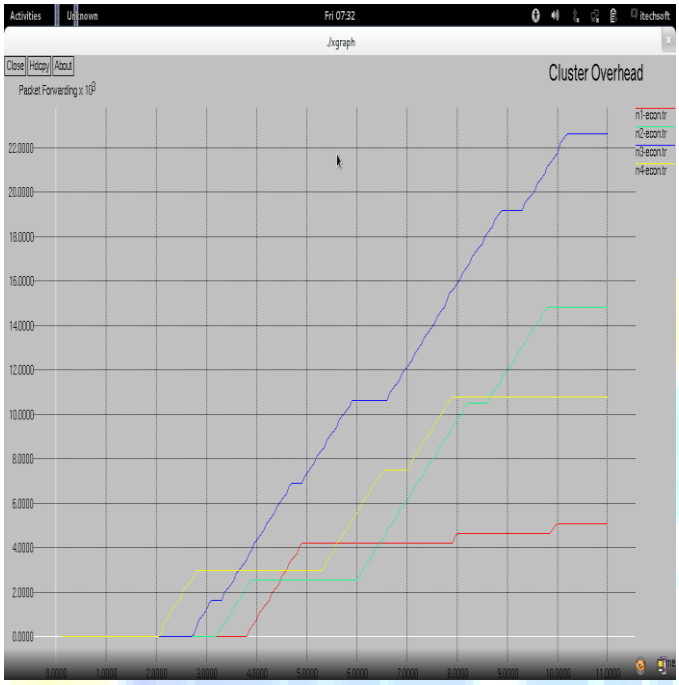

Fig.4. Energy Consumed

The figure above shows the energy consumed by four nodes. Since by using Elliptical curve Cryptography key size is reduced energy consumed is also less. This output is simulated by ns2.

V.CONCLUSION

Presented an approach which ensure the security of mobile users in mobile WiMAX. In this paper, we have investigated the security functionality of the EPA scheme has three security vulnerabilities, which will lead to DoS attacks and replay attacks. In order to overcome the vulnerability in the authentication process in handovers under the DoS and the replay

attacks and to improve the efficiency, we have proposed the EEP scheme using WPKI. The EEP scheme can reduce the handover delay, which is a huge bottleneck of the current handover process specified by the IEEE802.16e. We believe that the proposed scheme is both secure and efficient, which is qualified to be a competitive replacement of the current handover scheme.

REFERENCES

[1] IEEE 802.16-2004,"IEEE Standard for Local and Metropolitan Area Networks- Part 16: Air Interface for Fixed and Broadband Wireless Access Systems, "IEEE Press 2004.

[2] IEEE 802.16-2005,IEEE Standard for Local and Metropolitan Area Networks-Part 16:"Air Interface for Fixed and mobile Broadband Wireless Access Systems, "IEEE Press 2005.

[3] D. Q. Liu and M. Coslow, "Extensible authentication protocols for IEEE standards 802.11 and 802.16," 2008, pp. 1–9..

[4] A. M. Taha, A. T. Abdel-Hamid, and S. Tahar, "Formal analysis of the handover schemes in mobile WiMAX networks," in *Proc. 2009*

[5] V. Narayanan and L. Dondeti (2008, 09 December 2010), EAP Extensions for EAP Re-authentication Protocol (ERP).[RFC5296. Available: http://www.rfc-editor.org/rfc/rfc5296.txt.

[6] Y. Ohba, Q. Wu, and G. Zorn (2010, 09 December 2010), Extensible Authentication Protocol (EAP) early authentication problem statement.[RFC5836].

[7] L. Jong-Hyouk and C. Tai-Myoung, "Secure handover for Proxy Mobile IPv6 in next-generation communications: scenarios and performance,"

[8] C. Li, "Seamless mobility," M.S., Center for Information and Communication Technologies, Technical University of Denmark, 2006..

[9] Y. Xiao, "PKMv2: mutual authentication," in *WiMAX/MobileFi: Advanced Research and Technology*. Auerbach Publication, 2008, pp. 100–102.

[10] D. Simon, B. Aboba, and R. Hurst (2008, 09 December 2010), The EAP-TLS Authentication Protocol. [RFC5216].Available:http://www.rfceditor.org/rfc/rfc5216.txt

[11] G. Zorn (2010, 09 December 2010), RADIUS Attributes for IEEE 802.16 Privacy Key Management Version 1 (PKMv1) Protocol Support.[RFC 5904]. .

[12] Whitfield Di e and Martin E. Hellman.New directions in cryptography. IEEE Transactions on Information Theory, IT-22(6):644–654, 1976.

[13] Tetsuya Izu, Jun Kogure, Masayuki Noro, and Kazuhiro Yokoyama. Ecient implementation of schoof's algorithm. In ASIACRYPT '98: Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security, pages 66–79, London, UK, 1998.Springer-Verlag.

[14] Aleksandar Jurisic and Alfred J. Menezes. Elliptic curves and cryptography. Dr. Dobb's Journal,1997. [Len87] H. W. Lenstra. Factoring integers with elliptic curves. Annals of Mathematics, 126:649–673, 1987.

[15] C. Enrique Ortiz. An Introduction to Java Card Technology. 2003.

[16] Henna Pietil¨ainen. Elliptic curve cryptography on smart cards. 30 October 2000.

[17] Scott A Vanstone P. Van Oorschot, Alfred J Menezes. Handbook of Applied Cryptography. CRC Press, 1996

[18] Bruce Schneier. Applied cryptography (2nd): protocols, algorithms, and source code in C. John Wiley & Sons, Inc., New York, NY, USA,1995.[wik] Wikipedia.

Author's Detail:

Ancy Anna Mani doing her M.E in Communication System at PSN College of Engineering And Technology, Tirunelveli. She received her B.Tech in Electronics and Communication from Muslim Association College of Engineering, Trivandrum in 2011. Her research interests include wireless network, artificial intelligence.