Practical Approach for Improving Security in Wireless Mesh Network Through Ecc and Two Way Authentication Scheme

Avinash P. Wadhe
aviwadhe@gmail.com
Department of Computer Science & Engineering
G. H. Raisoni College of Engineering,
Nagpur.

N.A.Chavhan
niki.chavhan@gmail.com
Department of Computer Science & Engineering
G. H. Raisoni College of Engineering,
Nagpur.

ABSTRACT

Wireless Mesh Networks (WMNs) are multi-hop and multi-radio network in which each node communicates with each other to increase the performance of network and are new emerging wireless technology , potential for strengthening internet deployment and access. However, security is the main challenge in WMNs A well-performed security framework for WMNs will require to network survivability and strongly support the network growth. In this paper, we propose a secure, lightweight public key (two way authentication and Access Control based on Elliptic curve cryptography) based security scheme WMNs is to guarantee well-performed key management services and protection from unauthorized access. It is more scalable and requires less memory compared to symmetric key-based schemes. Furthermore, it is much more lightweight than other public key-based schemes such as RSA-based protocols have significant problems in terms of the bandwidth and storage requirements. Currently, the RSA algorithm requires that the key length be at least 1024 bits for long term security, however, it seems that 160 bits are sufficient for elliptic curve cryptographic functions.

Keywords

Elliptic curve Cryptography; security; two way authentication ;access control; wireless mesh networks

1. INTRODUCTION

The Wireless mesh networks (WMN) are multi-radio, multi-hop networks with the ability of dynamically self organizing and self configuring. They can automatically establish ad hoc networks and maintain mesh connectivity between them. WMN's diversify the abilities of ad hoc networks as they are composed of mesh routers and mesh clients. Mesh clients perform pure ad hoc behaviour by performing routing and self configuration. The mesh routers are the main addition, on top of providing a mesh of self-configuring and self-healing links among themselves [1][2]. They also provide a gateway functionality which enables integration with existing wireless and wired networks. A mesh router also contains additional routing functions to support mesh networking

Wireless Mesh Network is an application technology different from the traditional peer-to-peer wireless bridges it provides the multi-hop and multi-path connection to form a wireless environment of MESH framework so that the occurrence of single point failure can be prevented. Under the traditional mode of wireless bridge, if something wrong happens to just one of nodes, In this multi-hop wireless MESH network, any node can be connected to other nodes in a wireless way and delivered the packets from others. There are 3 types of components under the framework of Wireless Mesh Network:

MP (Mesh Point): Nodes in the mesh network, in charge of the delivery of the packets from each node.

MAP (Mesh Access Point): It works with the functions of middleware transmission in the mesh network.

MPP (Mesh Portal) : It plays as the bridge for interfacing two networks, usually connects the wired network with the wireless MESH network shown in figure 1 The architecture considered is the client wireless mesh network architecture which is comprised of mesh clients that provide peer to peer networks among client devices.

The main difference between mesh clients and mesh routers is that clients only have one wireless interface and less computational abilities.[3].With this infrastructure provides connectivity to other networks, routing abilities of clients provide improved connectivity and coverage within the mesh network

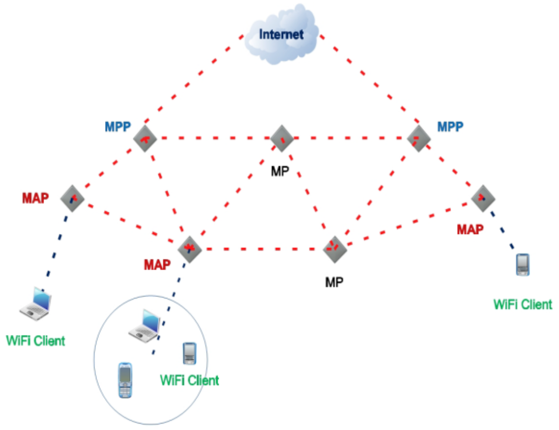


Figure 1: Typical Mesh Structure

The application of WMN, It constructs a wireless backhaul rapidly by using the MESH network in the areas that are not easy to wire. Especially for the temporary and short-termed working area, it can avoid the waiting time of applying for a least-line. Moreover in difficult environments such as emergency situations, tunnels, oil rigs, battlefield surveillance, high speed mobile video applications on board public transport or real time racing car telemetry wireless MESH deployment is very useful An important possible application for wireless mesh networks is VoIP. By using a Quality of Service scheme, the wireless mesh may support local telephone calls to be routed through the mesh. But security is main challenge for WMN and providing solution to the security challenges is a major research area in recent years in the fields of WMNs.

2. SECURITY ISSUES IN WMNS

Security issue in WMN cab identified by taking simple example Figure 2 shows a branch of a WMN where a mobile client (MC) is within the transmission range of TAP3(transit access point) and therefore relies on it to get Internet connectivity; the data generated and received by the MC goes through TAP1, TAP2, and WHS(wireless hotspot). Let us consider an upstream message (i.e., a message generated by the MC and sent to the Internet). Before this message reaches the infrastructure, several verifications need to be performed successfully. First of all, as Internet connectivity is a service for which (usually) the MC has to pay, TAP3 needs to authenticate the MC in order to perform the calculation correctly. This authentication can be done in different ways; for example, using symmetric key cryptography but implementation of it require battery efficient device MC is In fact, because the MC is battery operated, the authentication has to be energy efficient, which makes the use of public key cryptography primitives these primitives have a high computational overhead and are prone to DoS attacks.(misused by an adversary that can continuously ask the verification of a signature leads to drain battery)

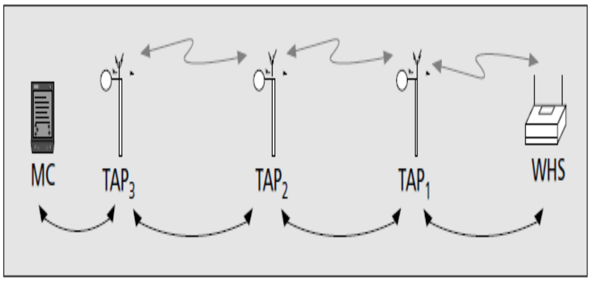


Figure 2: Example of Mesh network

Public key cryptography-based schemes are ideal to overcome these issues due to their high scalability, low memory requirements, easy key-addition/revocation for a new node, and no requirement of complicated key distribution. However, it is computationally expensive to apply public key cryptography to such a multi-hop network require such public key approach, which is more scalable and requires less memory compared to symmetric key-based schemes. More importantly, it should be more energy-efficient than existing public key-based approaches and practically feasible to implement it on mesh platforms.

3. RELATED WORK

Wireless mesh network is a multi-hop communication .All packet generate from source to target node in hop by hop forwarding manner .To ensure the authenticity of each node is very much essential and communication must be secure .There is reach literature available on key management and intrusion detection method which discussed about secure communication in multi-hop wireless mesh network .In Fahad T. Bin Muhaya, Fazl-e-Hadi, AtifNaseer [1] worked on selfish node detection in WMN by focusing routing information. Every node calculates field value from their neighbors .Every node has the information about neighbor’s field values sefish node. The node always forwards the packet having highest field value and hence the packet reaches to its destination. But not talk about scalable key management and proper authentication scheme.

M.Imani, M.E.Rajabi, M. Taheri, M.Naderi [5] proposed the Vulnerabilities in network layer at wireless mesh network gives the survey on The various Vulnerabilities are: Selective forwarding and Blackhole attack, Sinkhole attack, Sybil attack, Wormhole attack, Rushing attack. As all of the wireless networks suffer from much vulnerability and conclude that, the efficient method for preventing external attacker is cryptography with a globally shared key scheme.

ZHAI Min, HUANG Ting-Ieicode [5] proposed Public key infrastructure and Certificate authority (CA) which are very important authentication mechanisms. Because the wireless mesh network does not have pre established trusted network architecture, therefore, it is unrealistic to establish a central centralized CA. Problem encountered when the service node changes then information required re-distributed and old node will be a security risk. However, it is not easy for off-line CA to frequently re-distribute all the sub-secret of services nodes on account of heavy workload. Need proper and efficient protocol for authentication

Andreas Noack, Jorg Schwenk [7] proposed the application of group key agreement (GKA) protocols. They compare the performance of three group key agreement protocols in new model: Burmester-Desmedt I (BD1), Burmester-Desmedt II (BD2) and the Tree Based Key Agreement (TBKA) protocol. All of the chosen protocols support any positive number of mesh nodes greater than one. Under a cryptographic perspective, there are some slight differences in the security properties of the mentioned protocols but fail to give scalable key management.

In this paper implementation of elliptic curve cryptography for key generation and two way mutual authentication schemes for key management serve the purpose successfully.

4. BACKGROUND

In 1985 Victor Miller, who was then at IBM, and Neil Koblitz from the university of Washington first introduced the Elliptic Curve Public Key Cryptography system, a method based on the Discrete Logarithmic problem over the points on an elliptic curve. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead. The ECC has received considerable attention from mathematicians around the world, and no significant breakthroughs have been made in weaknesses in the algorithm.

4.1 Introduction to ECC Cryptosystem

Cryptographic applications require fast and precise arithmetic. So elliptic curve groups over the finite fields of $F_p$and $F_{2m}$are used in practice. The protocol described in this paper depends on the security of the elliptic curve primitive known as ECDH key generation function. This function utilizes the arithmetic of points which are elements of the set of solutions of an elliptic curve equation defined over a finite field.

Following are the Operations Used in ECC

1) Point: An ordered pair of scalars satisfying the elliptic curve equation is called a point, denoted as P(x,y).

2) Elliptic Curve Group: The set of solutions of the elliptic curve equation together with a special point called point at infinity form.

3) Point Multiplication: The Multiplication of an elliptic curve point P, by an integer e will be denoted by K*P.

It is equivalent to adding P to itself K times, which yields another point on the curve.

Elliptic Curve Cryptography (ECC) is a public key cryptography. The principal attraction of ECC compared to RSA is that it offers equal security for a far smaller key size, thereby reducing processing overhead. Consider wireless mesh network, where authentication scheme require less computation overhead. Basically ECC is based on algebraic structure of elliptic curve over finite fields. An elliptic curve over a finite field GF (a Galois Field of order P) is composed of a finite group of points (x_i, y_i) where integer coordinates xi, yi satisfy the long Weierstrass form:

y2 + a1xy + a3y = x3 + a2x2 + a4x + a6

4.2. ECC-BASED ACCESS CONTROL

An elliptic curve consists of the points satisfying the equation:

$$y^2 = x^3 + ax + b$$

Where x, y, a and b are elements in GF (P) (a *Galois Field* of order, where P is a prime).

Each choice of (a, b) yields a different elliptic curve. For example, Figure 2 shows an elliptic curve of

$$y^2 = x^3 + 7x$$

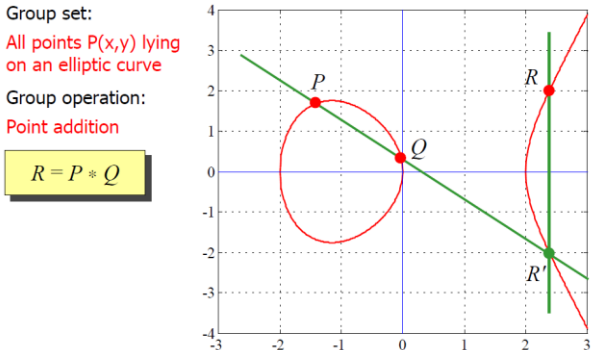


Figure 3: Elliptic curve and point addition

The elliptic curve group operation is closed under addition so that addition of any two points is also a point in the group. Given two points P (x_1, y_1) and Q (x_2, y_2), the addition results in a point R (x_3, y_3) given by:

$$(x_1, y_1) + x_2, y_2) = (x_3, y_3)$$

Such that

$$x_3 = \beta 2 + \beta + x_1 + x_2 + a$$

$$y_3 = \beta (x_1 + x_3) + x_3 + y_1$$

$$\beta = (y_1 + y_2) / (x_1 + x_2)$$

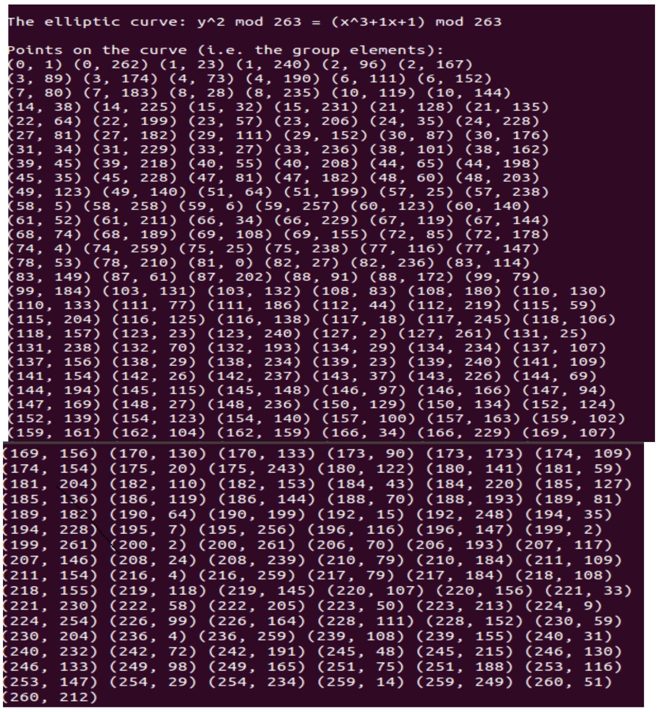
If P=Q, then R = P+P=2P. Addition of multiple points will give. ECC relies on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP), that is, given points P and Q of the group, it is very difficult to find a number K such as .Q=k × P.(hard problem).Values used for x ,y ,a and b are not necessarily real number instead they may have value from any field. Using real number for cryptography it is very much difficult to store in computer memory. Hence use of finite field is necessary. There are two types finite field (Galois Field)

4.2.1 ELLIPTIC CURVE OVER GF(P)

Let GF(p) be a finite field, p > 3, and let a, b ∊ GF(p) are constant such that $4a^3 + 27b^2 \equiv 0$ (mod p). An elliptic curve, $E_{(a,b)}$(GF(p)), is defined as the set of points (x, y) ∊ GF(p) * GF(p) which satisfy the equation $y^2 \equiv x^3 + ax + b$ (mod p) together with a special point, O, called the point at infinity.

4.2.2. Elliptic Curve over GF(2^m) for some m ≥ 1.

Elliptic curve E(a, b)(GF(2^m) is defined to be the set of points (x, y) ϵ GF(2^m) * GF(2^m) which satisfy the equation $y^2 + xy = x^3 + ax^2 + b$; where a, b ϵ GF($2^m$) and b≠0, together with the point on the curve at infinity, O. The points on an elliptic curve form an abelian group under a well defined group operation. The identity of the group operation is the point O.In this paper EC over **GF(2^m)** is not used as because extended bit-fiddling operation needed by binary curve are not required and binary curve are best for hardware application. Prime curve are best for software application. Following are the screenshot showing generation of Elliptic curve point. By taking P=263 and a=1, b=1



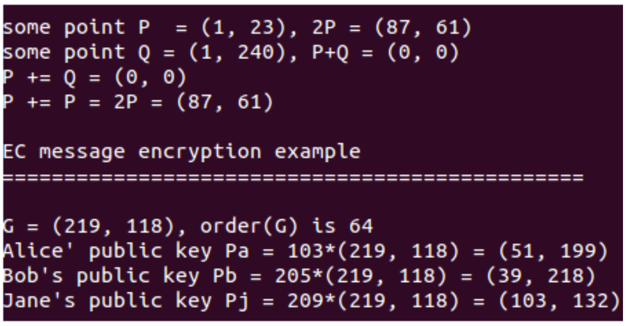
```
The elliptic curve: y^2 mod 263 = (x^3+1x+1) mod 263

Points on the curve (i.e. the group elements):
(0, 1) (0, 262) (1, 23) (1, 240) (2, 96) (2, 167)
(3, 89) (3, 174) (4, 73) (4, 190) (6, 111) (6, 152)
(7, 80) (7, 183) (8, 28) (8, 235) (10, 119) (10, 144)
(14, 38) (14, 225) (15, 32) (15, 231) (21, 128) (21, 135)
(22, 64) (22, 199) (23, 57) (23, 206) (24, 35) (24, 228)
(27, 81) (27, 182) (29, 111) (29, 152) (30, 87) (30, 176)
(31, 34) (31, 229) (33, 27) (33, 236) (38, 101) (38, 162)
(39, 45) (39, 218) (40, 55) (40, 208) (44, 65) (44, 198)
(45, 35) (45, 228) (47, 81) (47, 182) (48, 60) (48, 203)
(49, 123) (49, 140) (51, 64) (51, 199) (57, 25) (57, 238)
(58, 5) (58, 258) (59, 6) (59, 257) (60, 123) (60, 140)
(61, 52) (61, 211) (66, 34) (66, 229) (67, 119) (67, 144)
(68, 74) (68, 189) (69, 108) (69, 155) (72, 85) (72, 178)
(74, 4) (74, 259) (75, 25) (75, 238) (77, 116) (77, 147)
(78, 53) (78, 210) (81, 0) (82, 27) (82, 236) (83, 114)
(83, 149) (87, 61) (87, 202) (88, 91) (88, 172) (99, 79)
(99, 184) (103, 131) (103, 132) (108, 83) (108, 180) (110, 130)
(110, 133) (111, 77) (111, 186) (112, 44) (112, 219) (115, 59)
(115, 204) (116, 125) (116, 138) (117, 18) (117, 245) (118, 106)
(118, 157) (123, 23) (123, 240) (127, 2) (127, 261) (131, 25)
(131, 238) (132, 70) (132, 193) (134, 29) (134, 234) (137, 107)
(137, 156) (138, 29) (138, 234) (139, 23) (139, 240) (141, 109)
(141, 154) (142, 26) (142, 237) (143, 37) (143, 226) (144, 69)
(144, 194) (145, 115) (145, 148) (146, 97) (146, 166) (147, 94)
(147, 169) (148, 27) (148, 236) (150, 129) (150, 134) (152, 124)
(152, 139) (154, 123) (154, 140) (157, 100) (157, 163) (159, 102)
(159, 161) (162, 104) (162, 159) (166, 34) (166, 229) (169, 107)
(169, 156) (170, 130) (170, 133) (173, 90) (173, 173) (174, 109)
(174, 154) (175, 20) (175, 243) (180, 122) (180, 141) (181, 59)
(181, 204) (182, 110) (182, 153) (184, 43) (184, 220) (185, 127)
(185, 136) (186, 119) (186, 144) (188, 70) (188, 193) (189, 81)
(189, 182) (190, 64) (190, 199) (192, 15) (192, 248) (194, 35)
(194, 228) (195, 7) (195, 256) (196, 116) (196, 147) (199, 2)
(199, 261) (200, 2) (200, 261) (206, 70) (206, 193) (207, 117)
(207, 146) (208, 24) (208, 239) (210, 79) (210, 184) (211, 109)
(211, 154) (216, 4) (216, 259) (217, 79) (217, 184) (218, 108)
(218, 155) (219, 118) (219, 145) (220, 107) (220, 156) (221, 33)
(221, 230) (222, 58) (222, 205) (223, 50) (223, 213) (224, 9)
(224, 254) (226, 99) (226, 164) (228, 111) (228, 152) (230, 59)
(230, 204) (236, 4) (236, 259) (239, 108) (239, 155) (240, 31)
(240, 232) (242, 72) (242, 191) (245, 48) (245, 215) (246, 130)
(246, 133) (249, 98) (249, 165) (251, 75) (251, 188) (253, 116)
(253, 147) (254, 29) (254, 234) (259, 14) (259, 249) (260, 51)
(260, 212)
```

Figure 4: Result of ECC Point on Curve (y^2(mod p) = x^3+1x+1 mod p) and p=263

5. RESULT ORIENTED KEY GENERATION MODULE USING ECC

From above generated point, let select P (1,23) as a point and randomly select any integer from 1 to p -1
and d act as private key .Multiply d with point P in other words add point P with d times this point act as public key .as explain with below snapshot. So public key is (p, P, Q, n) and private key is d.



```
some point P  = (1, 23), 2P = (87, 61)
some point Q = (1, 240), P+Q = (0, 0)
P += Q = (0, 0)
P += P = 2P = (87, 61)

EC message encryption example
==============================================

G = (219, 118), order(G) is 64
Alice' public key Pa = 103*(219, 118) = (51, 199)
Bob's public key Pb = 205*(219, 118) = (39, 218)
Jane's public key Pj = 209*(219, 118) = (103, 132)
```

Figure 5: Result of ECC Key Generation

5.1. Elliptic Curve Diffie-Hellman Protocol (ECDH)

An example of ECC version of Diffie-Hellman

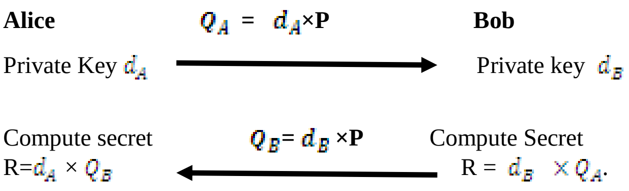


Figure 6: ECDH Key Exchange Protocol

6. TWKM: PROPOSED TWO WAY KEY MANAGEMENT SCHEME

To achieve the objective of developing a low-computational and scalable key management for WMNs, this proposed model will be carried out in the following steps:

6.1. TWO WAY Authentication and Access Control based on ECC

The first step is to establish key between nodes. To meet scalability requirements for a large number of mesh nodes, proposed a public key management scheme based on Elliptic Curve Cryptography (ECC). Compared to symmetric key cryptography, ECC is more scalable, requires lesser memory for storing keys, introduces low communication overhead, and is easy to deploy

6.2. Key Establishment

There is one or more trusted third-node on the network called Key Distribution Center (KDC) to generate all security materials (e.g. keys, certificates), issue and revoke user's access privileges. Note that this KDC is not required to be online all the time like in symmetric scheme [9]. Initially, KD selects a particular elliptic curve over a finite field GF(p) (where p is prime number) and publishes a base point with a large order q (where q is also a prime). It picks a random number d ∈ GP(p) as a private key for mesh node M_i and generates a corresponding public key Q_i = d_i× p .The key pair {d_i, Q_i}is then loaded to M_i It generates this key-pair based on p by itself since it is more powerful than a Mesh node. After this step, every node in the network has an ECC key-pair which will be used to establish secret (symmetric) key for secure communication. The proposed scheme is based on Elliptic Curve Diffie- Hellman (ECDH) [13] to establish a shared secret key between two nodes.

6.3. Authentication and Access Control Protocol

Generally A called *Alice*, or wants to access data from a mesh node or data on the coordination node. *Alice* obtains the base P from a KDC and generates her private key (**d_A**) and public key **Q_A = d_A×P KDC** issues a proper access control list ac_A notation used for protocol designing

Symbol	Description
IDA →	**Identifier of entity A**
x_{AB} →	**Shared secret key between A and B**
acA →	**Access control list issued to entity A**
signA (m)→	**Message m is signed by entity A**
A→ B : m →	**Entity A sends entity B a message m**
(m)K →	**Symmetric encryption of message m with key K**
MAC (K , m) →	**A message authentication code of message m with key K**
h(m) →	**Hashing value of message m**
|| →	**Concatenation**
TAP →	**Transit access point**

Table 1: Notation used in TWKP

TWKP protocol is described in Figure 6, which includes the following steps.

Step 1:

Alice selects a random number which r ϵ GF(p) will be used as a session key with C and S , creates a secret key L1= h(X_{CS} □ T_C) (T$_A$ where is the current timestamp generated by Alice), and encrypts r with the key rL Alice then signs this encrypted value along with its . Certificate **S1 = sign A((r)L || certA)** and send combination ***(r)L, TA, S1*** to mesh node B

Step 2:

After receiving the message from *Alice*, node C first checks if the timestamp T_A is valid (i.e. by verifying T_A < $T_{current}$ if where $T_{current}$ **is** current timestamp. Then it verifies *Alice'* signature. If valid, then *Alice* is authentic to C. *Alice's* certificate $cert_A$ is also verified to check the validity of the access list which was assigned to her. *Alice* is authorized if $cert_A$ is valid. Node C(KDC module) now construct the secret key L= h (X_{ac}

□ T_A) and decrypts (r)L to get r . It then generates a secret key M=$h(X_{CS}$ □ T_C)where T_C is the timestamp created by C, encrypts *r*, and builds a MAC value (i.e.MAC1= MAC(X_{CS} ,(r) M ||I D_A… Finally, C node sends (r)M,T_C ,IDA,MAC1 through TAP2 to B.

Step 3:
When B receives the message it checks T_C>$T_{current}$ Then it verifies MAC1Value if valid then Alice is authentic to C. then B calculate the secret key M=$h(X_{CS}$ □ T_C) and Decrypts (r)M to get r. then B builds MAC (MAC2=(r,ID_S)) and send to Alice from TAP2 to TAP1. Node B sends IDs to node C

Step 4:
Node C verifies MAC2 if valid it created signature S_C**=sign(I**D_s**||I**D_C**||**$cert_C$) and sends IDc, Ds ,Sc to Alice after receiving the IDc, Ds ,Sc from C. Alice Verifies C signature Sc if valid then S and C are authenticated with Alice.

7. SECURITY ANALYSIS

The security level of the proposed TWKP protocol depends on the security level of ECC signature, message authentication code (CBC-MAC), and encryption algorithm (RC5). According to literature, it has been proved for strong security frame work. So in this paper, we focus on possible vulnerabilities to the proposed protocol.

8. EXPECTED RESULT

Implementation of Elliptic curve proves that it has less computation overhead, which is remarkably improve the security to WMN and proposed TWKP scheme shows scalable key management .Due to use of two way authentication, various attack can be prohibited such as Denial of service attack, as it checks the validity of timestamp on mobile KDC module (Tc) If it not valid then it discard the message .Considering real scenario of WMN, TWKP protocol calculation of total time require for user authentication ,node authentication and total time for two way authentication will estimate remarkably less computational speed .As it will be implemented in next module of project.

9. CONCLUSION AND FUTURE WORK

With more and more applications coming out, the destination of this promising technology, saying WMNs, will be well-performed, secure, and wide-spread wireless connection. ECC-based access control scheme in wireless mesh network the protocol for the network to authorize a user to access the network. ECC has attracted much attention as the security solutions for wireless networks due to the small key size and low computational overhead. For example, 160- bit ECC offers the comparable security to 1024-bit RSA. Implementation of ECC on primary field performance will increase substantially; in future it is possible to further reduce the running time by using more refined and careful programming. Public-key cryptography is feasible for wireless mesh network security applications including access control. Implementing the tickets, self-generated pseudonyms, and the hierarchical identity-based cryptography, will help to achieve more desired security objectives and efficiency.

10. REFERENCES

[1] Fahad T. Bin Muhaya, King Saud University Fazl-e-Hadi AtifNaseer (2010), “Selfish Node Detection in Wireless Mesh Networks” . 201O International on Networking and Information Technology.

[2] Yatao Yang Ping Zeng Xinghua Yang Yina Huang (2010),“Efficient Intrusion Detection System Model in Wireless Mesh Network” Second International Conference on Networks Security, Wireless Communications and Trusted Computing

[3] Jinyuan Sun, Chi Zhang (2011), “SAT: A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks” ieee transactions on dependable and secure computing, vol. 8, no. 2,

[4] ZHAI Min, HUANG Ting-Iei (2010), “A RSA Keys harinScheme based on Dynamic Threshold Secret Sharing Algorithm for WMNs”. 978-1-4244-6837 9/10/$26.00 ©2010 IEEE

[5] M.Imani Bing He, S M.E.Rajabi M.Naderi (2010) “Vulnerabilities in network layer at Wireless Mesh Networks (WMNs) ”.International Conference on Educational and Network Technology (ICENT 2010)

[6] Bing He, Saugat Joshi, Dharma P. Agrawal (2010), “Group Key Agreement Performance in Wireless Mesh Networks”. 35th Annual IEEE Conference on Local Computer Networks LCN 2010, Denver, Colorado

[7] Andreas Noack J¨org Schwenk (2010), “Group Key Agreement Performance in Wireless Mesh Networks” 35th Annual IEEE Conference on Local Computer Networks

[8] Vipul Gupta, Douglas Stebila_, Stephen Fung Eberle “Speeding up Secure Web Transactions Using Elliptic Curve Cryptography”Sun Microsystems, Inc.2600 Casey Avenue Mountain View, CA 94043

[9] ANSI X9.63 (1999.), “Elliptic Curve Key Agreement and Key Transport Protocols”, American Bankers

[10] Li, X. Xin and Y. Hu, (2007) “Key management in ad hoc networks using self-certified public key system”, International Journal of Mobile Communications, vol. 5(1), pp. 94-106.

[11] S Mittra, “Iolus (1997,) a framework for scalable secure multicasting,” in Proceedings of ACM SIGCOMM’97, Canada, September, pp.14-18.

[12] F Lee and S. Shieh, (2004) “Scalable and Lightweight Key Distribution for Secure Group Communications,” International Journal of Network Management, 14:167-176.

[13] Y. Fu, J. He, R. Wang and G. Li, (2004) “A key-chain-based keying scheme for many-to-many secure groupCommunication,” ACM Transactions on Information and System Security (TISSEC), vol. 7(4), pp. 523 – 552.

[14] M S. Siddiqui, and C. S. Hong, (2007) “Security Issues in Wireless Mesh Networks”, Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE’07). New York IEEE Press, pp. 41−47.

[15] H. Mu and Y. Liu, (2006) “Mesh Based Multicast Key Management Scheme in Ad Hoc Networks,” in Proceedings of IEEE ICSP, pp.

[16] Patrick Longa, and Catherine Gebotys, “Efficient Techniques for High-Speed EllipticCurveCryptography” 2010 University of Waterloo, Canada

[17] Kossi Edoh“Elliptic Curve Cryptography on PocketPCs*” International Journal of Security and Its Applications Vol. 3, No. 3, July, 2009

[18] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation of“ Elliptic Curve Cryptography over Binary Fields”, 2000, Available at

[19] IEEE 802.11 Standard Group Web Site. Available:<http://www.ieee802.org/11/>.

[20] IEEE 802.15 Standard Group Web Site. Available: <http://www.ieee802.org/15/>.

[21] IEEE 802.16 Standard Group Web Site. Available:http://www.ieee802.org/16/

[22] IEEE Standard 802.1X-2004☹(2004) “Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control”, December 2004.

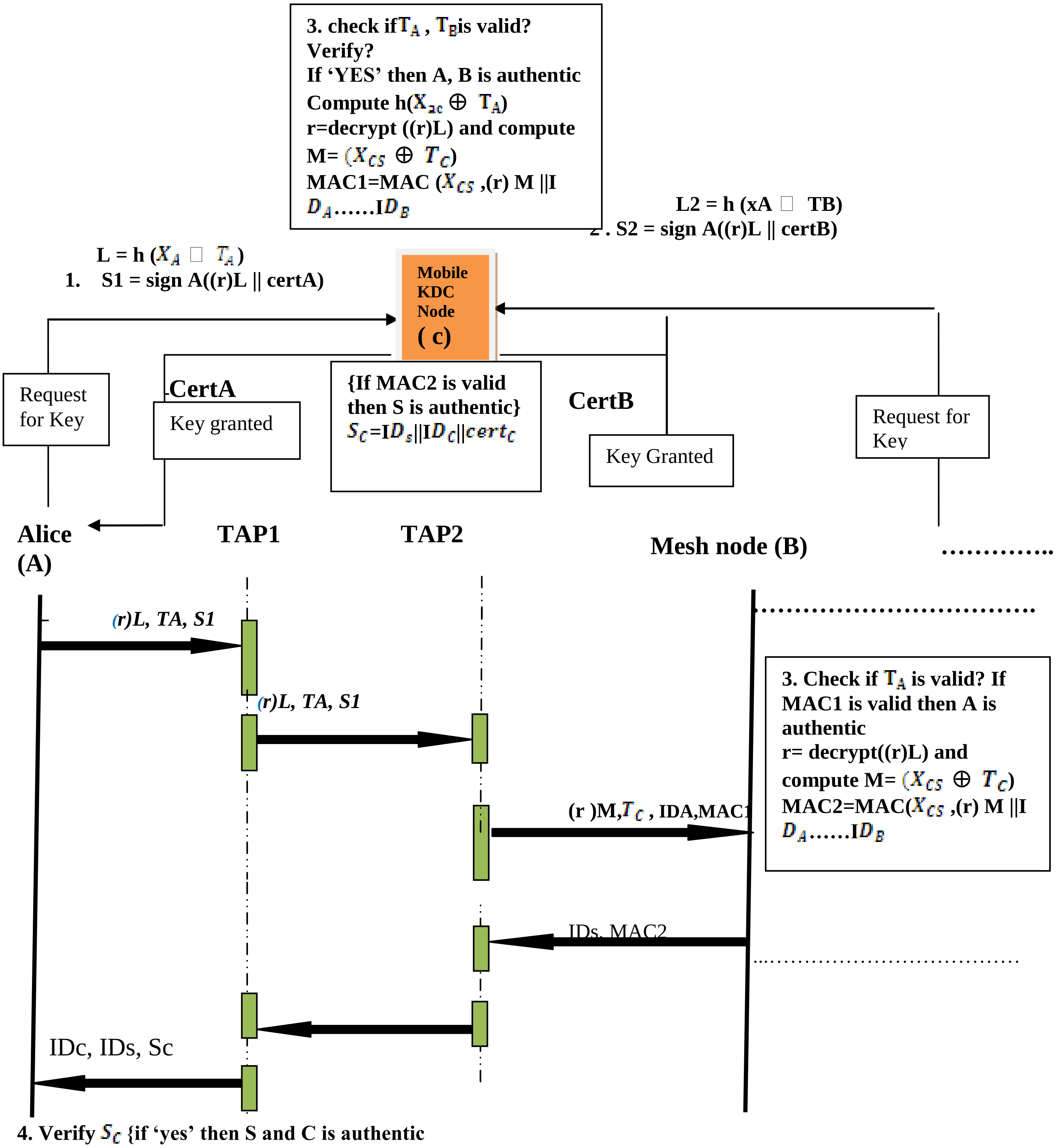

3. check if T_A , T_B is valid?
Verify?
If ‘YES’ then A, B is authentic
Compute h(X_ac ⊕ T_A)
r=decrypt ((r)L) and compute
M= (X_CS ⊕ T_C)
MAC1=MAC (X_CS ,(r) M ||I D_A……ID_B
L2 = h (xA □ TB)
2. S2 = sign A((r)L || certB)
L = h (X_A □ T_A)
1. S1 = sign A((r)L || certA)
Mobile KDC Node (c)
Request for Key
CertA
Key granted
{If MAC2 is valid then S is authentic}
S_C=ID_s||ID_C||cert_C
CertB
Key Granted
Request for Key
Alice (A)
TAP1
TAP2
Mesh node (B)
…………..
(r)L, TA, S1
(r)L, TA, S1
(r)M,T_C , IDA,MAC1
3. Check if T_A is valid? If MAC1 is valid then A is authentic
r= decrypt((r)L) and
compute M= (X_CS ⊕ T_C)
MAC2=MAC(X_CS ,(r) M ||I D_A……ID_B
IDs, MAC2
IDc, IDs, Sc
4. Verify S_C {if ‘yes’ then S and C is authentic

Figure 7: TWKM Protocol