SECRET SHARING SCHEME AND ELLIPTIC CURVE CRYPTOGRAPHY IN MANETS

V.Srikanth,N.ChaitanyaKumar
Sreenidhi Institute of Science and Technology, Hyderabad, India

Abstract: A self-organized mobile node wireless network without fixed infrastructure is mobile ad hoc network (referred MANET). Decentralization is practise of transferring power from one single master node to all other nodes. In order to remove such security threats as eavesdropping, monitoring, denial of service and routing attacks, this is achieved. Decentralization is ensured by the use of secret sharing techniques. MANET has a hidden key/public key pair that provides the public and every node with share of secret key. Nodes are spread across networkcausinga fast and unpredictable shift in its topology. New nodes can be connected to the network, while other nodes can (temporarily) exit or simply fail to connect at the same time as they move to the area not served by the network. A new node may approach other nodes to collect its confidential information and in particular, its share. Based on the type of scenario in which these keys are used, individual secret / public keys can be received. The first is popular PKI scenario: each node would independently generate its hidden / public key pairs. In order to jointly calculate a valid certificate binding node's identity to a public key, the node must then contact other nodes. This is where we use Elliptic Curve Digital Signature Algorithm (ECDSA).

Index: *Mobile Ad-Hoc Network, Secret Sharing Technique, Elliptic Curve Cryptography.*

1.INTRODUCTION

MANET, known as Mobile Ad hoc Network, is self-composed, complex, and infrastructureless system. A single node has its own signal transmission spectrum, and multiple nodes can communicate and share messages within the range. MANET includes freely moving nodes. New nodes join, and when they move out of MANET range, few nodes can leave or fail to connect.

MANET nodes are energy-restricted, i.e. the nodes are battery-operated machines. A variety of safety threats, such as snooping, routing attacks, denial of service and surveillance, are susceptible to MANETS.

Using digital signatures and public key cryptography to authenticate and encrypt, the Public Key Infrastructure (PKI) helps ensure secure contact. The distributed PKI approach to completely decentralise the MANET network is implemented in this paper.

In the PKI setting, where Certificate Authority (CA) issues and distributes public key certificates from related bodies, CA uses the master secret key to sign certificate. Generic PKI is not appropriate for MANET because due to its complex and changing topology, we cannot allocate CA's sole power to a single node; i.e., the CA node could break down or leave the MANET range, which ends up being inaccessible to CA.

To follow distributed PKI criterion for MANETS, we use a(t, n) threshold approach which leads to sharing of CA power. Therefore we supply MANET nodes with master secret key s.

Our proposal discusses how every node should be able to sign a certificate using Elliptical Curve Digital Signature Algorithm (ECDSA) and verify certificate with a threshold number of nodes.

1.1Attacks on MANETS

On MANETS, Passive and Aggressive are two kinds of attacks. Passive attacks intercept major travel information and aggressive attacks obstruct the network by interfering with the usual sequence of operations. Infected nodes provoke both aggressive and passive attacks. Ownership of the intruder over a legitimate node could also be affected. As network contains protocol levels, attacks on a layer are carried out specifically and the protection can also be run at the same level. As the mobile nodes communicate using a wireless medium, it is possible to listen to the messages sent or to add fake messages to

the physical layer. The attacker will begin traffic monitoring and traffic analysis attacks on account of one-hop communication retained among neighbours.

In order to generate routing hops plus network congestion in the network layer, attacker exploits routing algorithms. An infected node is used by the attacker to perform Denial of Service (DOS) and SYN flooding attacks via the transport layer. In device layer, worm attacks, mobile viruses and repudiation attacks are big attacks. Multiple levels, such as denial of service (DOS) and man-in-the-middle, perform a number of attacks.

In order to avoid a large amount of attacks, this paper proposes dissemination strategies by SecretSharing Scheme and Elliptic curve cryptography.

1.2Distributed PKI

A variety of services, including secrecy, transparency, verification, non-repudiation, encryption and digital signatures, are introduced by public key cryptography (PKC).

A Public Key Infrastructure (PKI) that is essential for implementation of public key cryptography is handling digital certificates. The certification contains the entity's public key and ID, master secret certificate credentials, and verified by master public key PK in the PKI environment scope. The certification authority (CA) issues and manages certificates for related organisations in the sense of the PKI environment.

In MANETS, it is hard to accept the same PKI, as network is also dynamically infrastructure-free. The portion of CA must then be allocated to nodes i.e. master secret key s must be split between the different nodes, and master secret key generated only ifdigit of secret shares thresholds is at least incorporated.

1.3Threshold Cryptography

Since MANET is decentralised network, PKI master secret key(s) is split into nodes using secret exchange schemes.Most popular and widely used method for secret sharing is Shamir secret sharing technique. The dealer shares in this scheme a secret with n users. Each user gets the dealer's share secretly. It takes (t, n), where t is required from n users, a threshold access to recreate the secret.Shamir's secret sharing can be used in MANET's. MANET's nodes themselves can also play the part of the dealer.

1.4Related work

To share position of CA or trusted authority is one of the common issues that MANET faces in the introduction of encryption; plans also use a secret distribution technique to spread CA or trusted authorities' secret keys to secure MANET. Zhou and Haas [6] first to suggest that localised CA was for MANETS. In the PKI case, threshold encryption was used to assign the Certification Authority (CA) role between selected servers. However this is not sufficient, as these nodes for a purely ad-hoc situation are not always available. Kong et al. [16] modified related principle to spread trust across all nodes. In special RSA threshold scheme [17] [18], however they have demonstrated uncertainty. The Shamir secret sharing [8] technique is most commonly used secret sharing technique. Shamir's secret sharing code and bi-variate polynomial use have been shown to help spread the secret of CA across all MANET nodes.

In Bi-variate polynomials have been used to allow new nodes to dynamically enter the network without any external trusted party being needed. Invention impacted by initial work [19]. Anzai et al. [20] and Herranz et al. [21] developed decentralised, exible, dynamic group distribution schemes by using polynomials in two variables. Aim for a shared community to build hidden group keys. Saxena et al. [22] used a novel approach to set up pair wise keys in non-interactive way for handheld ad-hoc scenario. Hanaoka et al. [27] developed a multi-user setup signature based on the BLS signature with good protection. Chaitanya et al. [15] have implemented node authentication using BLS Signature.

Our plan has a lot to do with the sales policies of MANET. The proposed MANET is completely self-managed and authenticates the ways in which connectivity is formed between nodes. The MANET distribution methods and the use of secretsharing and cryptography of elliptical curves can be found in our article.

The configuration of the node is constructed using the Elliptic Curve Digital Signature Algorithm. For MANET, this scenario is very significant as nodes are primarily resource constraint devices and it is difficult to afford high computational overhead demanded by large keys.

2.PRELIMINARIES

2.1 Self-Organized PKI and Secret Sharing Technique

The role of PKI is entirely distributed between MANET nodes by using secret shares for self-organized MANETS. The first to implement secret sharing techniques were Blakley and Shamir. The dealer and U set = $\{u_1,u_2,u_3, \dots ,u_n\}$ out of n users is a secret sharing scheme. The distributor has S information and must disclose them tou$_i$ user privately. A valid subset u (for: u ϵ U) can be used to recompile S's secret for at least 't' of users with valid shares. The t is assumed to be the number of thresholds, and known as threshold access structure (t;n). The Secret Communication Scheme of Shamir uses polynomial interpolation to construct structures for threshold access (t, n). Z_q to be a finite q > n field and keep it secret for S ϵ Z_q. In the most t-1 where P(x) is continuously S and all the other coefficients are chosen uniformly from the Z_q randomly and autonomously. That is,

$$P(x) = S + \sum_{i=1}^{t-1} a_i * x^i$$

Each ui user is associated publicly with an ai field element. Similar parties are connected to similar elements in the field. The dealer sends the value ui to the user in private, $[S]_i = P(a_i)$; for i = 1,…,n. We can presume without lack of generality group of parties ready to recover secret S is $P_1,\dots,P_t$. Secret S is obtained by $\sum_{i=1}^{t} l_i * [s]_i$ where $l_i=\prod_{j\neq i}\frac{a_j}{a_j-a_i}$is Lagrange coefficient. It is proven that no intelligence is delivered to any party of less than t parties, that is, because of their shares every secret is equally probable.

2.2 Elliptic Curve Cryptography

Elliptic curve Cryptography (ECC) is a public key cryptography originating from algebraic elliptical curves over finite fields. Elliptical curve ECC allows smaller keys to have equivalent protection, i.e. RSA, than non-EC encryption, so it is advised to use bigger keys to achieve greater security or stronger protection. The ECC is used for digital signatures, key agreements, pseudo-random generators, and other functions. An electronic record used to confirm public key possession is a public key certificate, also referred to as a digital certificate or identification certificate. The certificate contains the key, identity and digital signature of authority (called issuer) that has checked its contents. From elliptic curve cryptography, the ECDSA public key licence, signing keys and public keys are extracted. Although ECDSA relies on more efficient elliptical curve encryption, it requires smaller keys to ensure security equivalence and, eventually, to obtain the same results as other digital signature algorithms.

2.2.1 Signature Generation

Suppose Alice needs to give Bob a signed message. The curve parameter must first be decided (CURVE, G and n). Besides the field and curve equation, 'G' the base point of curve,' and 'n' is order of point 'G' are needed.

- Let hash of the message be "m" =z
- Select a random integer k
- Curve point (x1,y1)=k * G
- Select the private key dA
- Compute r=x1 mod n, if r=0 choose another value of k
- Evaluate $s = k^{-1}(z + r * dA)$, if s=0 choose another value of k
- Signature pair is (r,s)

2.2.2 Signature Verification

- Calculate $u1 = z * s^{-1} \bmod n$

- Calculate u2 = r * s^{-1}mod n
- Calculate Q_a=G*dA (Q_a public key)
- Calculate the curve point (x1; y1) = u1 * G + u2 * Q_a
- Calculate v=x1 mod n
- Signature is valid if v=r

3.OUR PROPOSAL

3.1 SETUP

Initial set N of L nodes (founding Nodes) which run the following protocol jointly are contained in MANET.

- The public parameters needed are: a prime order q, an additive group G, generated by a certain element P.
- Implementation requires e : G X G → GT an admissible bilinear pairing and two hash functions h:{0,1}* → Zq and H : {0,1}* → G which are collision-resistant and made public.
- Threshold value t is set. The safety desired for MANET is set by Threshold t and a necessary security condition is t ≤ L ≤N.
- Every node Ni ϵ N selects random bivariate polynomial Fi(x,z) ϵ Zq[x,z], with maximum degree t-1 of variables x and z, and symmetric of all variables of x and z implicitly.

  F(x, z) = $\sum_{N_i \epsilon N}$ Fi(x, z).

  Let fi,0 = Fi(0, 0) and s = $\sum_{N_i \epsilon N}$ fi, 0= F(0; 0)
- Every Ni ϵN node secretly sends to each of other Nj ϵ N founding nodesFij = Fi(x,h(Nj)) polynomial and includes value Yi = fi,0P
- When each node in N finishes in the previous step, each founding node Nj ϵ N will compute its final secret , a univariate polynomial

$$S_j(x) = \sum_{N_i \epsilon N} F_{ij}(x) = \sum_{N_i \epsilon N} F_i\left(x, h(N_j)\right) = F(x, h(N_j))$$

- The public key PK and secret key SK of MANET are determined from information obtained from rest of the founding nodes.

  PK = sP = $\sum_{N_j \epsilon N} f_{i,0} P = \sum_{N_j \epsilon N} Y_i$

  The corresponding secret key is SK = s = F(0; 0) any founding N_j node can evaluate from ones partial information S_j (x), a share $[s]_j = S_j(0) = F(0, h(N_j))$ of secret key SK= s.

  If new N_m node wants join the MANET. The following protocol must be implemented:
- Nm chooses the group NM of nodes for which Nm will associate at least t existing. It presents as Nm and asks that the nodes in NM be integrated into MANET
- If the $N_j \epsilon N_M$ node allows N_m node into the MANET, the polynomial is secretly sent to Nm

  $S_j(h(N_m)) = F(h(N_m), h(N_j)) = F(h(N_j), h(N_m)) = S_m(h(N_j))$
- As N_m Node collects information from t various nodes, the secret $S_m(x)$ polynomial can be obtained by using Lagrange interpolation.
- Lastly N_m node will calculate the share of the $[s]_m = S_m(0)$ Secret key SK = s of the MANET.

3.2Key Generation

As every node partial secret s_i has been obtained, the RSA key generation protocol is run by nodes. A public pair (pk_i) and private (sk_i) key pair are generated by this Protocol. All other nodes n_i have a private key (pk_i) kept confidential, and a public key (pk_i) available to other nodes. The public pk_i key for encryption of messages to nodes, key used for decrypting messages and signing of messages with its private key ski is done by node n_i

3.3Signature Generation Protocol

Node has two secret keys - MANETS' partial secret key s_i and secret key sk_i, partial secret key is used to sign a certificate partially and all the t-nodes must be signed to produce certificate which is completely signed. If node needs public key certificate, the neighbouring nodes are asked to establish partial signatures on certificate binding n_i// pk_i. If (t-1) partial signs are received by node n_i, then the node itself will produce a partial sign with its partial share, so now node has t partially signed values, then uses LaGrange's interpolation to combine.

- $P_i = H(m) * s_i$ where s_i share of each user and H(m) is hash of message "m".
- Point (shm) is

  shm = $\sum_{i\epsilon t} p_{i*} L_i$ Here L_i is LaGrange's Coefficient. $L_i = \prod_{p_j \in t, j \neq i} \frac{(0-h(N_j))}{(h(N_j)-h(N_i))}$
- Initially the nodes must agree on curve parameters like Elliptic curve field and equation, base point of elliptic curve(G), integer order of the base point(n).
- Let the message be shm
- Select random integer k
- Evaluate the point (x1, y1) = k * G
- Here dA is private key
- Compute r=x1 mod n, If r=0 select another k value
- Calculate s = k1(shm + r _ dA), If s=0 select another k value
- The signature pair is (r,s)

Each node now receives the certificate as mentioned above.

3.4Signature Verification Protocol

Any n_j node can verify n_i nodes certificate by using protocol below.

The n_j node has following n_i nodes information:

- Signed node certificate n_i (shm)
- MANET Public Key (PK) and value P.
- ID and Public key of the node n_i (N_i//pk_i)

The n_j Node is used to check the certificate with the Elliptical Curve Digital Signature Algorithm:

- Evaluate u1 = z * s^{-1}mod n
- Evaluate u2 = r * s^{-1}mod n
- Compute Qa = G * dA
- The curve point obtained is (x1; y1) = u1 * G+u2 * Qa
- Calculate v=x1 mod n
- Signature is verified if v=r

If true certificate is valid, else invalid.

3.5 Cryptographic Operations

- As the (Public Key, Private Key) Key pair for each Node is Generated using RSA, nodes can communicate the messages by Encryption and Decryption.
- Encryption: The message(M) will be encrypted by receiver's Public key(e,n) ,Cipher value(C) is obtained.

$C = mod(M; n)^e$

- Decryption: The Cipher value(C) is decrypted using receiver's Private key (d,n) ,Decrypted value obtained is the Original Message.

$M = mod(C; n)^d$

3.6 EXAMPLE

- **Setup**

- The initial nodes are N_M = {N 1; N 2; N 3; N 4}

Number of Nodes = 4

- Public Parameters :

Prime order of the additive group G is q = 4019.

- Elliptic curve is E(F4019) : $y^2 = x^3 + 1$

- P = E(3198,578) is the Generator

- Let degree of polynomials (t=>2) and Field of Polynomials (k=>67)

- The two collision resistant hash functions - HTP (Hash to Point) : $\{0; 1\}^* \rightarrow G_2$ and HTR(Hash to Range) : $\{0; 1\}^* \rightarrow G_1$ Where HTP hashes an elliptical curve group G2 with the message given, and HTR hashes the message given for group G1.
- Every node selects symmetric-bivariate polynomial in GF(67) at random

$N1 = 3x^2z + 3z^2x + 8xz + 5z + 5x + 5$

$N2 = 5x^2z + 5z^2x + 3xz + 8z + 8x + 9$

$N3 = 8x^2z + 8z^2x + 5xz + 3z + 3x + 6$

$N4 = 2x^2z + 2z^2x + 4xz + 8z + 8x + 4$

- Implicit polynomial is F (x, z) = N1 + N2 + N3 + N4 defined by all nodes

$= 18x^2z + 18xz^2 + 20xz + 24x + 24z + 24$

- F(0,0) = 24 is MANET's secret (s)
- Each node secretly sends to each other the univariate polynomial $F_{ij} = F_i(x; h(N_j))$.
- Hash values of the Nodes are

Hn_1 = HTR("Node1"; k) = 1

Hn_2 = HTR("Node2"; k) = 6

Hn_3 = HTR("Node3"; k) =51

Hn_4 = HTR("Node4"; k) = 10

- The values below are sent to other nodes through each node:
- N1 includes Y1 = 5 * P = (152,1437)

$N11 = 3x^2 + 16x + 10$

$N12 = 18x^2 + 27x + 35$

$N13 = 19x^2 + 42x + 59$

$N14 = 30x^2 + 50x + 55$

- N2 includes Y2 = 9 * P = (409,2266)

$N21 = 5x^2 + 16x + 17$

$N22 = 30x^2 + 5x + 57$

$N23 = 54x^2 + 34x + 15$

$N24 = 50x^2 + 2x + 22$

- N3 includes Y3 = 6 * P = (3063,3143)

$N31 = 8x^2 + 16x + 9$

$N32 = 48x^2 + 53x + 24$

$N33 = 6x^2 + 28x + 25$

$N34 = 13x^2 + 49x + 36$

- N4 includes Y4 = 4 * P = (3863,2497)
  $N41 = 2x^2 + 14x + 12$

  $N42 = 12x^2 + 37x + 52$

  $N43 = 35x^2 + 54x + 10$

  $N44 = 22x^2 + 47x + 17$

- The secret univariant polynomial of all nodes is then determined by the values received.
  $S1(x) = 18x^2 + 62x + 48$

  $S2(x) = 41x^2 + 55x + 34$

  $S3(x) = 47x^2 + 24x + 42$

  $S4(x) = 46x^2 + 14x + 63$

- PK = s * P is Public key

= 24 * E(3198,578) = E(2651, 2267)

- Public key should also be equal to Y1 + Y2 + Y3 + Y4

=E(152,1437)+E(409,2266)+E(3063,3143)+E(3863,2497) = E(2651, 2267)

- The proportion of each nodes share from Si(0) is determined.

Shares of the nodes are

S1 = 48; S2 = 34; S3 = 42; S4 = 63

- These shares are verified by the following polynomial by substituting the hash value of nodes.

f(z) = F(0,z) = 24 _ z + 24

- If N5 wants to join MANET, it must identify and seek approval of three additional nodes. {N1;N2;N3}

Hn_5 = HTR("Node5"; k) = 52

- The following values are given to N5

S15 = 48

S25 = 34

S35 = 42

- N5 uses Lagrange interpolation to compute its secret univariate polynomial S5(x) = 24 _ x + 24

Generation of keys

- A particular key pair is determined accordingly by each node:

Node_1 = [(89,649),(189,649)]

Node_2 = [(17,321),(25,321)]

Node_3 = [(63,115),(7,115)]

Node_4 = [(91,202),(11,202)]

Signing

- The secret key component of each node is used as a secret key for signing in MANETs

S1 = 48; S2 = 34; S3 = 42; S4 = 63

- By linking Id with PK, every node creates a certificate

m_1='Node_1'+'89'+'649'

m_2='Node_2'+'17'+'321'

m_3='Node_3'+'63'+'115'

m_4='Node_4'+'91'+'202'

- Each node will then swap partial signatures to test the fully signed certificate.
    - If Node 1 requires its certificate to be computed (m1='Node1' +'89' +'649'), it asks the partial signatures of Node 2, Node 3 and Node 4.
    - Hm_1 = HTP(m_1) = E(2292; 106)
    - The partial signatures of Nodes 2, 3 and 4 are

    p2 = (Hm_1) * s2

    p3 = (Hm_1) * s3

    p4 = (Hm_1) * s4

    - Using Lagrange's Interpolation shm1=E(2132,2364).

    In order to sign using ECDSA the message must be integer value; we convert the point to integer value by

    z = shm1 mod 67 = 55

    - Select a random integer k=8
    - Select the private key d_a=17
    - The Elliptic curve used is E(F4019) : $y^2 = x^3 + 1$
    - The base point is A=E(2598,728) (x1,y1)
    - Calculate r=x1 mod 67=29
    - Calculate $s = k^{-1}(z + r * da)$ = 35
    - The signature pair is (r,s)=(29,35)

Signature Verification

- Calculate $u\_1 = z * s^{-1} \bmod 67 = 59$
- Calculate $u\_2 = r * s^{-1} \bmod 67 = 64$
- Calculate $Q_a = A * d_a$=(1807,1481)
- Compute the curve point (x1; y1) = u_1 * A + u_2 * Q_a =(2508; 1645)
- Calculate v=x1 mod 67=29
- Signature is verified if v=r
- Communication of message after verifying
- Each node's public and private key pairs

    Node_1 = [(e_1,n_1),(d_1,n_1)]=[(89,649),(189,649)]

    Node _2 = [(e_2,n_2),(d_2,n_2)]=[(17,321),(25,321)]

    Node _3 = [(e_3,n_3),(d_3,n_3)]=[(63,115),(7,115)]

    Node _4 = [(e_4,n_4),(d_4,n_4)]=[(91,202),(11,202)]

Message (M)= 55

- If Node 2 needs to send message to Node 4 , the message of Node will be encrypted using Public key of Node 4 and the message will be sent to Node 4.
- C=Encrypt(M,e4,n4) C = $\bmod(55; 202)^{91}$ Encrypted Value C = 127
- Node 4 obtains a cipher value and uses the private key of Node 4 to decrypt the code.

  M=Decrypt(C,d4,n4) M = $\bmod(127; 115)^{11}$after Decryption Value is M=55

CONCLUSION

A new MANET's certification system has been introduced based on decentralised PKI. There is a secret feature of our system in the MANET nodes and each node will choose its own private and public keys. Node authentication is achieved by means of a public key in the certificate. The credential operates via the Elliptic Curve Digital Signature Algorithm. It is possible to use this system to perform such MANET functions, such as exchanging verification and threshold operations in subgroup nodes, etc.

REFERENCES

1. F. Anjum and P. Mouchtaris, Security for wireless ad hoc networks. Wiley-Blackwell, Mar. 2007.
2. Vanesa Daza, Javier Herranz, Paz Morillo, Carla R`afols, Cryptographic techniques for mobile ad-hoc networks, Computer Networks, Volume 51, Issue 18, 19 December 2007, Pages 4938-4950.
3. Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on demand routing protocol for ad hoc networks. In Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (Mobicom 2002), September 2002.
4. Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of IEEE Infocom 2003, April 2003.
5. S. Kent and T. Polk. Public-key infrastructure (x.509) (pkix) charter. http://www.ietf.org/html.charters/pkix-charter.html.
6. L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network 13 (6) (1999) 24–30.
7. G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, American Federation of Information, Processing Societies Proceedings, vol. 48, 1979, pp. 313–317.
8. A. Shamir, How to share a secret, Communications of the ACM 22 (1979) 612–613.
9. Seung Yi and Robin Kravetso. Moca : Mobile certificate authority for wireless ad hoc networks. In The second annual PKI research workshop (PKI 03), Gaithersburg, 2003.
10. Dan Boneh, Ben Lynn, and Hovav Shacham (2004). "Short Signatures from the Weil Pairing". Journal of Cryptology. 17: 297–319.
11. Djenouri, Djamel, L. Khelladi, and N. Badache. "A survey of security issues in mobile ad hoc networks." IEEE communications surveys 7.4 (2005): 2-28.
12. Stallings, William (1990-05-03). Cryptography and Network Security: Principles and Practice. Prentice Hall. p. 165. ISBN 9780138690175.
13. Jack Doerner, Yashvanth Kondi, Eysa Lee, abhi shelat. "Threshold ECDSA from ECDSA Assumptions: The Multiparty Case" "2019 IEEE symposium on security and privacy".
14. Marc Green and Thomas Eisenbarth. "Strength in Numbers: Threshold ECDSA to Protect Keys in the Cloud"
15. N Chaitanya Kumar, Abdul Basit, Priyadarshi Singh, V. Ch. Venkaiah, and Y. V. Subba Rao. "Node Authentication Using BLS Signature in Distributed PKI Based MANETS" "International Journal of Network Security Its Applications (IJNSA) Vol.9, No.4, July 2017"
16. H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, URSA: ubiquitous and robust access control for mobile ad hoc networks, IEEE/ACM Transactions on Networking 12 (6) (2004) 1049–1063.
17. M. Narasimha, G. Tsudik, J.H. Yi, On the utility of distributed cryptography in P2P and MANETs: the case of membership control, in: Proceedings of ICNP'03, 2003, pp. 336–345.
18. S. Jarecki, N. Saxena, J.H. Yi, An attack on the proactive RSA signature scheme in the URSA ad hoc network access control protocol, in: Proceedings of the SASN'04, 2004, pp. 1–9.
19. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-secure key distribution for dynamic conferences, in: Proceedings of Crypto'92, LNCS, vol. 740, Springer-Verlag, 1993, pp. 471–486.
20. J. Anzai, N. Matsuzaki, T. Matsumoto, A quick group key distribution scheme with entity revocation, in: Proceedings of Asiacrypt'99, LNCS, vol. 1716, Springer-Verlag, 1999, pp. 333–347.

21. V. Daza, J. Herranz, G. S´aez, Constructing general dynamic group key distribution schemes with decentralized user join, in: Proceedings of ACISP'03, LNCS, vol. 2727, Springer- Verlag, 2003, pp.464–475.
22. N. Saxena, G. Tsudik, J.H. Yi, Efficient node admission for short-lived mobile ad hoc networks, in: Proceedings of ICNP'05, 2005, pp. 269–278.
23. Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." Annual International Cryptology Conference. Springer Berlin Heidelberg, 2001.s
24. Daxing Wang, Jikai Tang. "E_cient Aggregate Signature Algorithm and Its Application in MANET". In: International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering. vol. 7, No: 11, 2013.
25. Adul Basit, N Chaitanya Kumar, V. Ch. Venkaiah, Salman Abdul Moiz, Appala Naidu, Wilson Naik "Multi-stage Multi-secret Sharing Scheme for Hierarchical Access Structure." In International Conference on Computing, Communication and Automation (ICCCA), 2017 IEEE International Conference.
26. Hanoka G, Shuldt J.C.N, "On signatures with tight security in the multi-user setting" (2017) in : Proceedings of 2016 International Symposium on Information Theory and Its Applications, ISITA 2016, art. no. 7840392, pp. 91-95.