Multilevel Security Model using Distributed Keys in MANET

Neha Agrawal
Student
FET, Mody Institute Of Technology & Science, Laxmangarh(Sikar)

Sourabh Singh Verma
Assistant Professor
FET, Mody Institute Of Technology & Science, Laxmangarh(Sikar)

ABSTRACT

In military areas where MANET is used, enemy can physically capture soldier mobile device and can use stored private key to sign unauthorized messages. To overcome this security issue Shamir's (t, n) threshold secret sharing scheme is used to protect stored private key. Using this scheme the user private key is decomposed into 'n' parts and distributed to 'n' nodes in network. So when user wants his private key to sign message he just requests 't' or more key shares from any 't' out of 'n' nodes to reconstruct private key. But t-1 shares can't reconstruct the private key. Also, for securing the bandwidth and resources in MANET Shamir identity based cryptosystem and signature scheme is used, where a unique user identity is used as public key for encryption and decryption of messages. So, there is no requirement of certification and distribution of public key. We are proposing this security model for a Two tier ad hoc network architecture.

General Terms

Internet Security, RSA, Two tier Ad-Hoc Network

Keyword

Digital Signature, ID Based Signature scheme, MANET, Secret Sharing Scheme

1. INTRODUCTION

Today Mobile Ad hoc network (MANET) is being used in military operations for providing communication between soldiers. It is also being used to help in avoiding accidents and traffic jams in the road transportation system. Because of the node mobility features in MANET, it is very difficult to keep such a network secure. The three main mechanisms that are used to secure MANET are prevention, detection and response mechanisms. Prevention can be achieved by authenticating users to secure network against external attacks. Detection and response mechanisms secure network against internal attacks. The proposed technique in this paper mainly secure MANET against external attackers.

In military areas, as the scope of Mobile Ad-Hoc Network [1] increases the need for secure data communication also increases. Nodes in MANET store private key in their system database for signing secret messages or for decryption of encrypted messages. There is a big security issue regarding the protection of these stored private keys in soldier mobile device because it is vulnerable to physical capture attack by enemy. Enemy uses stored private key in soldier system to sign any illegal data or for decryption of secret data on behalf of soldier.

To secure private key in MANET it is necessary to decompose the private key into multiple shares and store each share at different places instead of storing it at one place. Shamir's (t, n) threshold secret sharing scheme [2] decompose the secret data into n pieces in such a way that combination of t or more pieces jointly recover data but less than t pieces can't recover the data. In the proposed scheme, the private key of user is decomposed into n shares by Key Generation center (KGC) or core node and KGC distribute each share to n nodes in the corresponding ad-hoc network. When any user wants to sign message, he request t or more private key shares from any t or more out of 'n' nodes and combine these obtained shares to recover the private key. After using the private key user delete this key from his system so that if system is compromised attacker can't forge it. Some papers like [3] provide priority among flows in MANET but key distribution is not included.

It is also necessary to secure public key along with private key. The previous techniques need certification of public key from PKI (Public Key Infrastructure). But the issue and verification of public key certificates creates overhead in MANET. Shamir's identity based public key scheme [4] is introduced to remove the need of public key certification from PKI. A unique identity of user like e-mail address or phone number etc is used as public key. The security lies in the fact that there is no requirement to send or certify (by PKI) public key because anyone who knows identity of user can encrypt or decrypt messages using this identity. This is beneficial for MANET because it saves network bandwidth and resources as there is no issuing and verification of certificates involved. So, in the proposed scheme KGC uses user identity as public key to generate private key for that user.

We are proposing this security model for a Two tier ad hoc network architecture [5] [6] [7]. In this architecture the ad hoc network is connected to the internet through a fixed access point. This access point is connected to fixed computer system. This fixed computer system act as KGC (Key Generation Center)for the corresponding ad-hoc network that comes in range of access point at that time. Any mobile node (in ad hoc network)can request its private key from this KGC.

The remainder of the paper is structured as follows: In section II related work is discussed. In Section III, Threshold secret sharing scheme is given. In Section IV, identity based public key cryptosystem is discussed. In Section V, the proposed security model is discussed. In Section VI, security analysis of the proposed model is given. In section VII, appendix is given. In section VIII, conclusion is given.

2. RELATED WORK

Researchers in paper [8], combines identity based cryptosystems threshold signature scheme & cannot consider any Trusted central authority. So, for implementing this scheme they used a distributed master key pair generation scheme prior to generating user private key shares because there is no central authority to generate user private key shares. This paper assumes a WVMN(Working Virtual Monitoring Node) node that acts as a central node for that Ad-Hoc group, & is responsible for generation and distribution of keys. But this distributed master key pair generation scheme and selection of WVMN node creates a unnecessary communication overhead in Ad-Hoc network that wastes MANET bandwidth and resources.

Researchers in paper [9], proposes a distributed key management and authentication scheme by using identity-based cryptography and threshold secret sharing. They proposed this scheme for a MANET without any assumption of pre-fixed trust relationship between nodes, each node in the ad hoc network provide the key generation and key management service, which effectively solves the problem of single point of failure in the traditional public key infrastructure (PKI)-supported system. But here also they use the distributed master key pair scheme that increases the unnecessary communication overhead.

Researchers in paper [10], also combines identity based scheme with threshold secret sharing scheme but uses it in two different scenarios; in the first scenario they assume the serving nodes as fixed nodes, in the second scenario theyassume the serving nodes as mobile nodes. This scheme provides authentication, confidentiality, & have reduced computation cost, & also avoid central control but again the use of distributed master key pair scheme creates unnecessary overhead.

So for minimizing the communication overhead generated due to the distributed master key generation scheme a security scheme is proposed by combining threshold secret sharing scheme and identity based signature scheme but for a two tier Ad-Hoc network architecture, Because in this architecture there is no need to apply distributed master key pair generation scheme as there is a centralized KGC or gateway that holds the master key for generating keys for user.

3. THRESHOLD SECRET SHARING

In Shamir's secret sharing scheme[2], instead of storing the whole secret in one place the secret is decomposed into 'n' parts and distributed to 'n' members randomly. Anyone who needs to reconstruct the private key back can request it from at least 't' or more members. The 't' members can be chosen randomly. But t-1 members can't create the original key. Here is the general case of threshold secret sharing scheme [2]:

1). Start with a secret 'm', 'n' a desired number of shares and a threshold value 'k', where all three values are integers and k is greater than equal to 2 and less than equal to n as shown in equation (1) [2]:

$$2 \leq k \leq n \quad \ldots\ldots(1)$$

2). Choose a prime 'p' bigger than both 'm' and 'n'

3). Choose a random polynomial of degree k-1 as given in equation (2) [2]:

$$q(x) = m\,x^0 + a_1\,x^1 + \cdots + a_{k-1}x^{k-1} \quad \ldots(2)$$

by choosing the coefficients 'a_i' uniformly and at random from the interval from 0 to p-1 inclusive. Here, a_0= m.

4). Compute 'n' shares as points (x_i , $q(x_i)$) on the graph of q(x) (The 'x' coordinates do not have to be consecutive integers, but no 'x' coordinate can be zero, since that would immediately reveal the secret.). These shares are distributed securely to each of the 'n' nodes [2].

5). If any 'k' users get together with their shares, they know 'k' distinct points on the polynomial's graph, and so the users can compute the polynomial's coefficients, including the constant term, which is the secret [2].

To calculate the polynomial from the shares *Lagrange interpolation formula* is used [2]:

A polynomial q(x) of degree k-1 is uniquely determined by k points, (x_i , y_i) for i is greater than equal to 1 and less than equal to k as shown in equation (3):

$$1 \leq i \leq k \quad \ldots\ldots(3)$$

assuming that the x_i's are all distinct. The polynomial is given by the formula as shown in equation (4) [2]:

$$q(x) = \sum_{i=1}^{k} \left(\prod_{1 \leq j \leq k\,,\, j \neq i} \frac{x - x_j}{x_i - x_j} \right) \quad \ldots\ldots(4)$$

Here, the Greek ∑(sigma) means to add up terms obtained by setting i = 1,2,…..,k. Similarly, the greek ∏(pi) means to multiply terms. The computations are all done in Z_p, that is mod p. By substituting x = 0 in equation (4), the equation becomes as given below in (5) [2]

$$q(0) = m = \sum_{i=1}^{k} y_i\,x_i \quad \ldots\ldots(5)$$

4. IDENTITY BASED PUBLIC KEY CRYPTOSYSTEM

In 1985, Shamirintroduced the concept of an identity-based (ID-based) cryptosystem [4] to simplify the public-key authentication problem. In this system, each signer needs to register at a private key generator (PKG) and identify himself before joining the network. Once a signer is accepted, the PKG will generate a secret key for that signer based on the signer's identity, which may include the signer's name, email address, etc. The signer's identity will be the signer's public key. In this way, a signer only needs to know the ''identity'' of his communication partner and the public key of the PKG, to verify a digital signature or to send an encrypted message. There is no public key directory needed in this system. The four steps involved are given below:

4.1 PKG keys

The PKG chooses its public and private key pairs as follows

i. Runs the probabilistic polynomial algorithm to generate two randomlarge primes, p and q.

ii. Chooses a random public key 'e' such that :

$$\gcd(e, \varphi(n)) = 1 \text{.....(6)}$$

and computes the private key using equation (7) [4]:

$$d = e^{-1} \% \varphi(n) \text{.....(7)}$$

4.2 Signer secret key generation

In this algorithm, the signer gets a copy of his secret key from the PKG through a two-step process as follows

i. A signer submits his identity i to the PKG.The PKG, with its private key d and the corresponding public key e, signs i by generating a secret key g, as given in equation in (8) [4]:

$$g = i^d \% n \text{.....(8)}$$

where g is the secret key of the signer.

4.3 Message signing

To sign a message m, the signer with the secret key g and the corresponding public key e of the PKG signs a message m by generating a signature pair $\sigma = (t, s)$ as follows:

i. Selects a random number r and computes t using equation (9) [4]:

$$t = r^e \% n \text{.....(9)}$$

ii. For the same random number r, computes s using equation(10) [4]:

$$s = g.r^{H(t,m)} \% n \text{.....(10)}$$

$\sigma = (t, s)$ is the complete signature of message 'm'.

4.4 Message verification

The identity-based signature $\sigma = (t, s)$ of a signer with identity 'i' is valid if and only if the following equality given in equation (11) [4] holds:

$$s^e = i.t^{H(t,m)} \% n \text{.....(11)}$$

5. PROPOSED WORK

When a new node joins the network each node register itself at KGC through following steps:

5.1 Phase 1: user private key generation & distribution

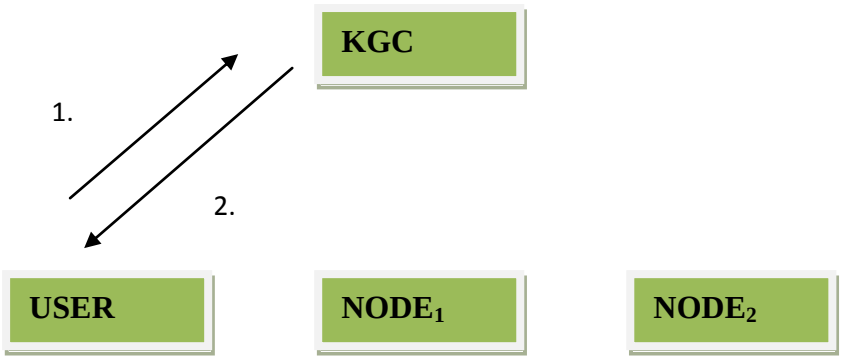
5.1.1 Key generation

5.1.1.1 KGC Public/Private keys

The KGC generates its public and private keys using RSA [12] [13] algorithm by following two steps

i. Randomly chooses two large primes numbers, p and q and computes n=p*q.

ii. Chooses a random public key 'e' such that:



1).Registration Request: $E[PU_{KGC}[ID_1||MAC_{ID1}||ID_{KGC}||N]]$
Where N=1(Request for registration)
2). KGC-Ack: $E[PR_{KGC}[ACK ||N]]$

Figure 1(a):User Registration phase at KGC

$$\gcd(e, \varphi(n)) = 1 \text{.....(12)}$$

and computes the private key using equation (13) [12][13]:

$$d = e^{-1} \% \varphi(n) \text{.....(13)}$$

5.1.1.2 User private key generation

The user at registration phase submits his identity to KGC. KGC generate private key using Shamir identity based signatures scheme[4]. The steps involved are

i. User submit his identity ID_i to KGC.
ii. KGC, generate private key for user using his own private key 'd' and identity ID_i of that user as given in equation (14) [4]:

$$PR_{ID_i} = ID_i^{\,d} \% n \text{.....(14)}$$

Where, PR_{IDi} is the private key of user and ID_i is the public key of user. The User-KGC communication scenario for User private key generation is shown in Figure 1(a).

5.1.2 Construction and distribution of user private key shares

5.1.2.1 Creating 'n' shares of user private key 'PR_{IDi}'

KGC create 'n' shares of User private key PR_{IDi} using threshold secret sharing scheme [2]:

i. Start with a secret 'PR_{IDi}', 'n' a desired number of shares and a threshold value 't', where all three are integers and t is greater than equal to 2 and less than equal to n as shown in equation (15) [2]:

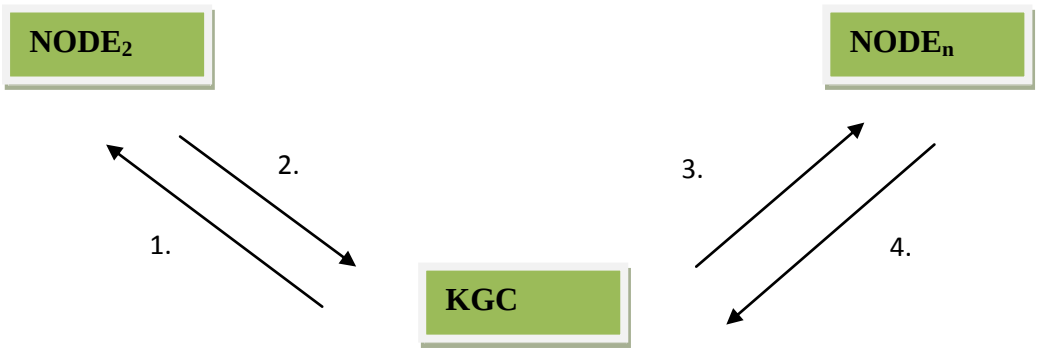
$$2 \leq t \leq n \text{.....(15)}$$

ii. Choose a prime 'p' bigger than both 'PR_{IDi}' and 'n'.

iii. Choose a random polynomial of degree t-1 as given in equation (16) [2]:

$$q(x) = m\,x^0 + a_1\,x^1 + \cdots + a_{t-1}x^{t-1} \text{.....(16)}$$

By choosing the coefficients 'a_i' uniformly and at random from the interval from 0 to p-1 inclusive. Here, m= PR_{IDi}.



1. **Distribute Share $S_{1,2}$:** $E[PU_{node2}[ID_{KGC}||ID_{node2}||ID_1||MAC_{ID1}||MAC_{KGC}||S_{1,2}]]$
2. **Node2-ACK:** $E[PR_{node2}[ID_{KGC}||ID_{node2}\ ||ACK]]$
3. **Distribute Share $S_{1,n}$:** $E[PU_{noden}[ID_{KGC}||ID_{noden}||ID_1||MAC_{ID1}||MAC_{KGC}||S_{1,n}]]$
4. **Noden-ACK:** $E[PR_{node2}[ID_{KGC}||ID_{noden}\ ||ACK]]$

Figure 1(b): Private key shares distribution

Figure1:Registration Phase

iv. Compute 'n' shares as points (x, $q(x_i)$) on polynomial 'q'.

*5.1.2.2*KGCdistribute the private key shares of user to other node's. The KGC communication scenario with other node's for distribution of User private key shares is shown in Figure 1(b).

5.2 Phase 2: user private key shares request and private key reconstruction

For signing data User send request for 't' private key shares to any 't' nodes. On receiving shares user can reconstruct the private key from shares using Lang range interpolation formula**.**

5.2.1 Private key shares request

The communication scenario between User-Other nodes for private key shares is shown in Figure 2.

*5.2.1.1*User broadcast request for private key shares to its neighbor nodes.

*5.2.1.2*When request is received by neighbor nodes, node's check whether they have private key shares for this user, if they have shares then nodes send these shares to user.

5.2.1.3 When user receive at least 't' or more shares, he reconstruct the private key using Lagrange's interpolation formula. Otherwise, user again send request for these shares to its neighbor nodes and then these nodes send request to its neighbors if they have not these shares.

5.2.2 Private key reconstruction

*5.2.2.1*When 't' or more shares are received by user then user uses Lang range's interpolation formula to reconstruct the private key as given in equation (17) [2]:

$$q(x) = \sum_{i=1}^{t} \left(\prod_{1 \le j \le t, j \ne i} \frac{x - x_j}{x_i - x_j} \right) \text{.....(17)}$$

And By substituting x = 0 in equation (17), the equation becomes as given in equation(18) [2]:

$$PR_{ID_i} = m = q(0) = \sum_{i=1}^{t} y_i \, x_i \text{.....(18)}$$

The original private key for User is PR_{IDi}.

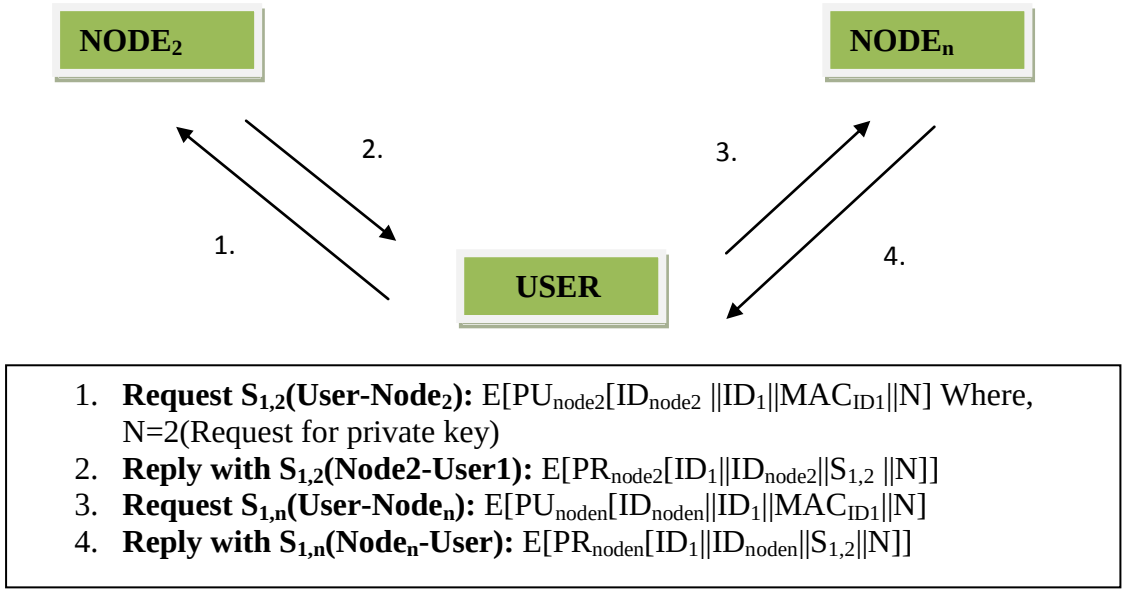


Figure2: Request for private key shares

5.3 Phase 3: signature generation

To sign a message 'm', the User with the secret key PR_{IDi} and the corresponding public key 'e' of the KGC signs a message 'm' by generating a signature pair $\sigma = (t, s)$ as follows:

5.3.1. Selects a random number 'r' and computes t using equation (19) [4]:

$$t = r^e \% n \quad \text{.....(19)}$$

5.3.2. For the same random number 'r', computes s using equation (20) [4]:

$$s = PR_{ID_i}.r^{H(t,m)} \% n \quad \text{.....(20)}$$

$\sigma = (t, s)$ is the complete signature of message 'm'.

5.3.3. User sends the signature $\sigma = (t, s)$ to the verifier. The communication scenario is shown in Figure 3.

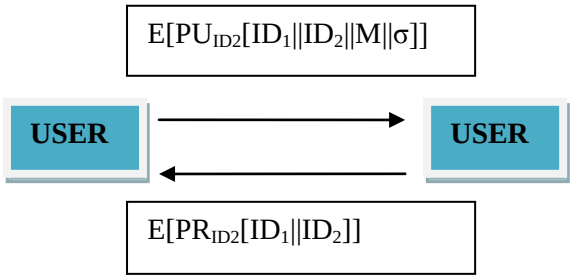


Figure 3:Signature Generation

5.4 Phase 4: signature verification phase

The identity-based signature $\sigma = (t, s)$ of a signer with identity 'ID_i' is valid if and only if the following equality as given in equation (21) [4] holds:

$$s^e = ID_i.t^{H(t,m)} \% n \quad \text{.....(21)}$$

6. EXPERIMENTALRESULTS &ANALYSIS

The proposed security scheme is implemented using Netbeans 7.0.1 in java. A Testbed is created by using 7 PC's. From these 7PC's 1 PC is a Desktop & other 6 are Laptop's. An access point is connected to fixed PC. And an Ad-Hoc Network is created between these 6 Laptops. We have assumed that all 6 Laptops are within the range of this access point. The Desktop with access point act as a Key Generation Center for the Ad-Hoc Network in its range. At each PC a

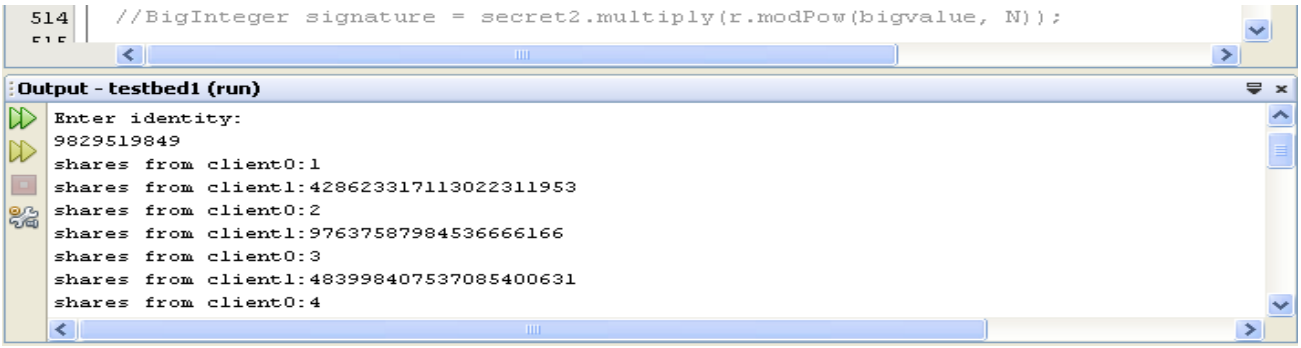


Figure 4: User enters its identity & receive shares from 5 clients

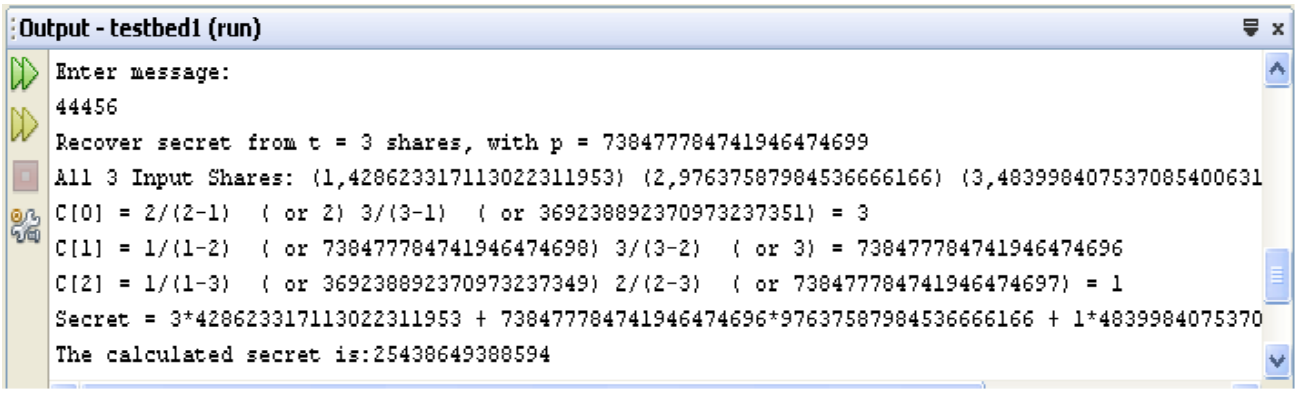


Figure 5: User reconstruct private key using received shares

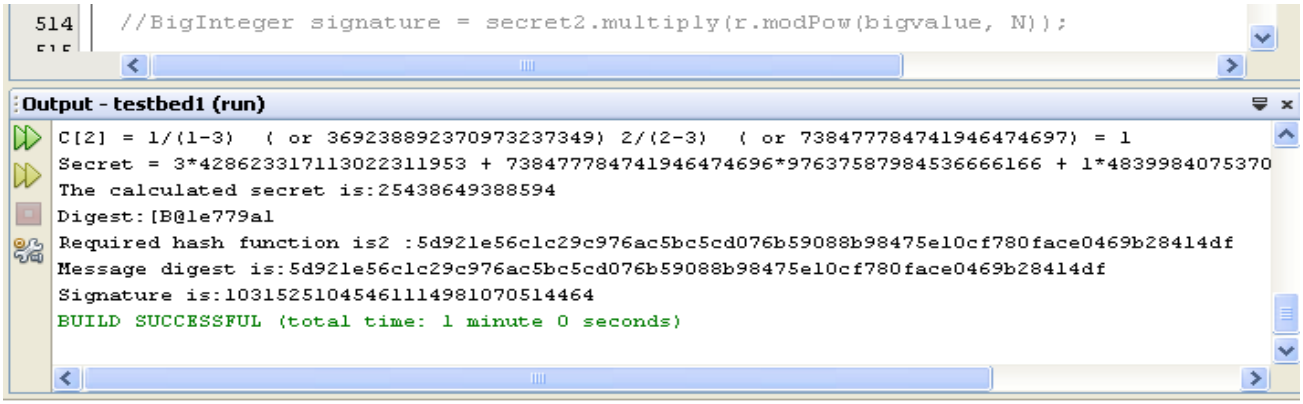


Figure 6: User generate signature using reconstructed private key

UDP (User Datagram Protocol) program is running for transmitting and receiving datagram packets from each other.

The Steps involved in the proposed technique are:

1. First User enters its identity and sends a request to KGC as shown in figure 4.
2. KGC construct the public key from this user identity using Identity Based Signature Scheme.
3. KGC computes 5 shares of private key using threshold secret sharing & distribute to 5 nodes in Ad-Hoc Network.

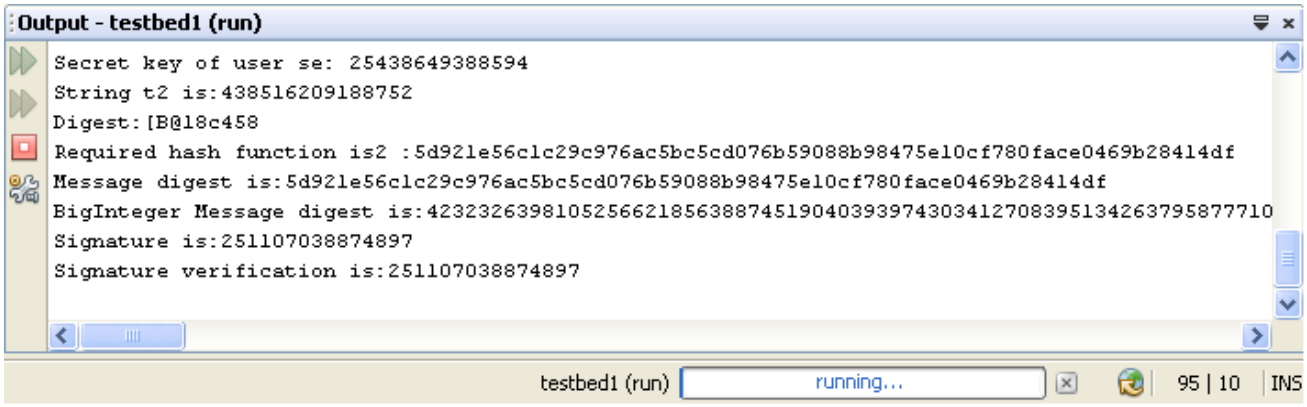


Figure 7: Receiver verify the received signature

4. User request private key shares from 5 nodes & on receiving shares as shown in Figure 4 &reconstruct the private key as shown in Figure 5.
5. User create signature using the reconstructed private key on secret message& send it to receiver as shown in figure 6.
6. On receiving signature along with message receiver verify the signatures as shown in figure 7.

The proposed security model is secured against following attacks:

1). If any attacker physically capture user PC in military areas where MANET is used then private key of user is still secure as it is distributed to other nodes.

2). Because here, the identity based signature scheme is used so, there is no need to use public key certificates and no exchange of public key between sender and receiver is required.

3). The proposed technique also provides confidentiality and authentication service as digital signatures are used.

4). The proposed also reduces the communication overhead generated in previous techniques [8][9] due to the use of distributed master key generation because a fixed KGC is used for a temporary period of time.

5). The proposed technique is secured against single point of failure as the Key Generation Center is used only at the initial phase (when node first join network) after that there is no use of KGC as the communication is done between nodes in MANET.

7. APPENDIX

Table 1: Notations Used

PARAMETER USED:	**DISCRIPTION:**
PR_{IDi}	Private Key of User i.
$S_{i,j}$	Private key share 'S' of User 'i' distributed to KGC 'j'.
ID_i	Identity/Public key of User 'i'.
PU_{KGCi}	Public key of KGC i.
PR_{KGCi}	Private key of KGC i.
E	Encryption
N	Showing request category: N=1(Request for registration) N=2(Request for private key share)
M	Message
MAC_{IDi}	Machine Authentication code of user with ID_i
MAC_{KGCi}	Machine Authentication code of KGC_i

8. CONCLUSION

This proposed work secure private key of user against attacker when the mobile device of that user is physically captured. Also the public key is also secured as user need to transmit this public key to receiver, because user identity is known to the trusted receiver. Also this security scheme has less communication overhead as compared to other techniques that use distributed master key pairing scheme, because here a KGC(Gateway in two tier ad-hoc network) distribute the private key. This scheme is good for applications where two tier ad-hoc network architecture is used.

9. ACKNOWLEDGMENTS

I would like to take this opportunity to express my deep sense of gratitude and profound feeling of admiration to Mr. Sourabh Singh Verma, Assistant professor, FET, Mody Institute Of Technology& Science for his guidance, inspiration and constructive suggestions. He provided me with lot of information and ideas regarding this.

10. REFERENCES

[1] Joseph P. Macker, M. Scott Corsen, Mobile Ad Hoc Networking and the IETF, Mobile Computing and Communications Review, Volume 2, Number 1.

[2] A.Shamir,1979,"How to Share a Secret," Communications of the ACM, Vol. 22, No. 11, pp. 612-613.

[3] Sourabh Singh Verma, Saroj Kr. Lanka, R.B.Patel, 2012, "Precedence Based Preemption and Bandwidth Reservation Scheme in MANET", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 2.

[4] Shamir A 1985., "Identity-based cryptosystems and signature schemes" In: Blakley GR, Chaum D, editors. Advances in cryptology: proceedings of crypto '84. Lecture Notes in Computer Science, vol. 196. Berlin: Springer-Verlag;,p. 47–53.

[5] M.Michalak, T. Braun,2005 , "Common Gateway Architecture for Mobile Ad-Hoc Networks, " Proc. of the Second Annual Conference on Wireless on-Demand Network Systems and Services (WONS'05) Volume 00, pp 70-75.

[6] Yuan Sun Elizabeth, M. Belding-Royer, Charles E. Perkins,2002, Internet Connectivity for Ad hoc Mobile Networks, International Journal of Wireless Information Networks, Special Issue on Mobile ad hoc Networks(MANETs): Standards, Research, Applications , pp 75-88.

[7] Khaleel Ur Rahman Khan, Prof. A Venugopal Reddy, Rafi U Zaman,2009, An Efficient Integrated Routing Protocol for Interconnecting Mobile Ad Hoc Network and the Internet, International Journal of Computer and Electrical Engineering, Vol. 1, No. 1, 1793-8198.

[8] Aasia Samreen and Seema Ansari,2009, "Certificateless ID-based Authentication using Threshold signature for P2P MANETs", IEEE .

[9] Deng H. Agrawal D,2004, "TIDS: threshold and identity-based security scheme for wireless ad hoc networks," Ad Hoc Networks 2 (3), pp 291-307.

[10] Shubat S.Ahmeda,2011, "ID-Based and Threshold Security Scheme for ad hoc Network", IEEE.

[11] William Stallings,2006, Cryptography And Network Security,Pearson Education.

[12] Behrouz A. Forozan, 2007, Cryptography and Network Security,Tata McGraw-Hill.