International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

A Cryptographical Approach for security in Mobile Adhoc Networks

R. Prasanna[1], K. Balaji[2]

[1]Department of Electronics & Communication Engineering Department of Electronics & Communication Engineering

[2]Mailam Engineering College Mailam Engineering College, Mailam 604304 Mailam 604304

Abstract: ***Adhoc network is very popular due to their infrastructure less architecture. One main challenge in such networks is to provide security in communication where the hosts rely on each other to keep the network connected. This type of network suffers in passive eavesdropping, impersonation, replay attacks. To resist this type of attack we use secret sharing techniques based on CRT. In this paper we have proposed a two level key distribution scheme for adhoc networks. In the first level we use Knapsack algorithm for key distribution among the cluster heads and in the second level we use Chinese remainder theorem (CRT) to share the secret among the nodes of the cluster.***

Keywords: Authentication, Knapsack-public key cryptography, Asmuth-bloom secret sharing, Chinese remainder theorem (CRT)

1. Introduction

In cryptography secret sharing is an interesting field that hides the secret by distributing it among group of people. It makes that the secret is not hidden but scattered around users. Amount of secret given to a participant is called shares. Access structure defines the structure in which the secret is to be distributed and combination of participants need to reconstruct the secret. Secret is distributed according to the function defined in access structure. After secret is distributed in *n* no of participants and recombination for secret need minimum *t* no of participants. This *t* is defined as threshold. Concept of secret sharing was firstly given by Adi Shamir [1] and Blakley [2] in 1979. Both proposed their work independently and they were using different method. Shamir secret sharing scheme was based on polynomial function and Lagrange's interpolation. While Blakley work on affine hyper plane. CRT based method reduce the high exponential cost of decryption process. Most important of them are Mignotte's scheme and Asmuth-Bloom scheme .

Adhoc network refers to infrastructure less network where all device are at equal status and can freely communicate to any other device on this network. As these networks follow decentralized architecture, hence it is very difficult to establish a secret key between the nodes. Because of its distributed nature and lack of centralized infrastructure, public key cryptography and certification is difficult to implement. Since it is a infrastructure less network so if some nodes are out of their signal range or absent due to sudden disconnection the combination of whole node will affected. Threshold secret sharing scheme will solve this problem.

There are many architecture proposed for the authentication in adhoc network. We have considered cluster based architecture to establish secure communication. Each cluster consists of a group of nodes called cluster node and a cluster head. In any cluster, cluster node will be able to communicate to each other with wireless communication. But when it wants to communicate to another network or rest of the network it has to communicate through base station. This base station will work as gateway. From the base station to the cluster heads the communication is infrastructure based. Thus we divide the architecture in two levels and propose two different key distribution strategies for these two levels to distribute the shares in their participants. In the first level we use Knap-sack public key generation algorithm for key distribution among the cluster heads and in the second level we use Chinese remainder theorem (CRT) secret sharing scheme to share the secret among the nodes of the cluster.

2. Related Work

Concept of secret sharing was firstly given by Shamir [1] and Blakley [2] independently. Both scheme was ideal secret sharing scheme. Simmons [3] has described multilevel access structure where each participants are assigned a level as a positive integer and the access structure is defined as those subset at least *r* participant all of level atmost*r*. This was approved by Brickel [4] who proposed a linear algebra based a generalized method for constructing ideal secret sharing scheme at multilevel and compartmented access structure. Two line of work in secret sharing has been discussed by Farras and Padro [8] for the construction of ideal secret sharing scheme and characterizing the ideal access structure. Iftene [6] described the use of generalized secret sharing based on CRT method in e-voting. Harh and Fuyou [9] propose the multilevel threshold secret sharing based on Chinese remainder theorem. A survey on the authentication technique based on threshold technique were given by Azer[7] and also described some challenges to be consider . A distributed key management and authentication approach by using ID-Based cryptography and threshold secret sharing was given by Mukherjee and Agarwal[5]. Third party Authentication scheme using Kerberos for mobile adhoc network was given by Gharib, Kaml and Belloulata[10].

3. Proposed Work

This paper proposes for the hierarchical access structure for authentication in adhoc network. Architecture is designed in

two levels. First level is for connection of root node to cluster head and second level is for connection of cluster head to cluster node. In this hierarchical network let there are *N* no of clusters. Each cluster may have different no of nodes in it. Because of this condition each cluster head will separately calculate and distribute its key among their cluster node. After deployment at level 1, Cluster head is wirely connected with root node and at level 2, Cluster node is in infrastructure less connection with cluster head.

Assumption

Root node and cluster head are trusted node. All the nodes along with cluster head and root node are synchronized. There is no overlapping between clusters i.e. clusters at level 2 are disjoint in nature. From root node to cluster head there is a infrastructure based communication. From cluster head to cluster node and among cluster node there will be infrastructure less communication

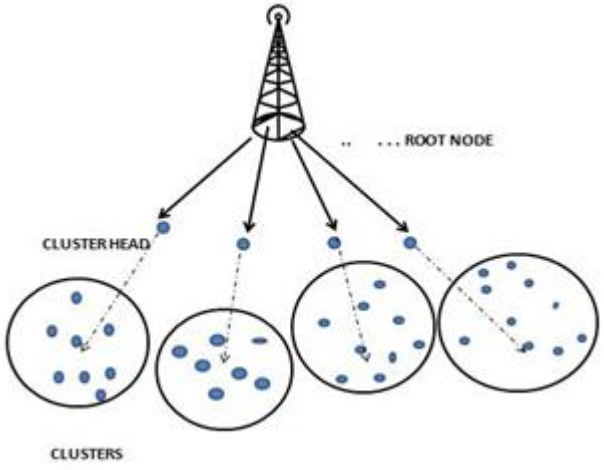

Figure 1: Key distribution Architecture

A. level 1 (Root node to cluster head)

This connection is assumed to be wired. Root node generates pair of public keys using asymmetric key generation. It will take *n* tuples super increasing key series. Where *n* is equals to the no of cluster head to which the key is to be distributed. Each tuple will be given to a single cluster head. This tuple will be the key for cluster head node and to be distributed among their participants.

1) Key generation at root node

Asymmetric key are generated by knapsack public key cryptography:

For *N* cluster head we choose n tuple super increasing series of *N* natural number.

$$w = (w_1, w_2, w_3, \dots\dots\dots\dots\dots, w_N)$$

Randomly select a integer such that

$$q > \sum_{i=1}^{N} w_i \quad (1)$$

And selects such that

$$1 \le r \le q - 1$$

And

$$\gcd(q, r) = 1$$

And now calculate

$$\beta_i = r w_i \bmod q \quad (2)$$

So the calculated series

$$\beta = (\beta_1, \beta_2, \beta_3, \dots\dots\dots\dots\beta_n)$$

Permute the series and find new series

$$\gamma = (\gamma_1, \gamma_2, \gamma_3, \dots\dots\dots\dots, \gamma_n)$$

This series will be the public key and series

$$w = (W_1, W_2, W_3, \dots\dots\dots\dots, W_n), q, r$$

Will be the private key. This private key tuples will be distributed to the cluster

2) Key Reconstruction

For reconstructing the key all the cluster node should be present there with their share. Thus here the threshold $t = n$. By collecting the tuples from all the cluster head, root node will again create a*N* tuple key

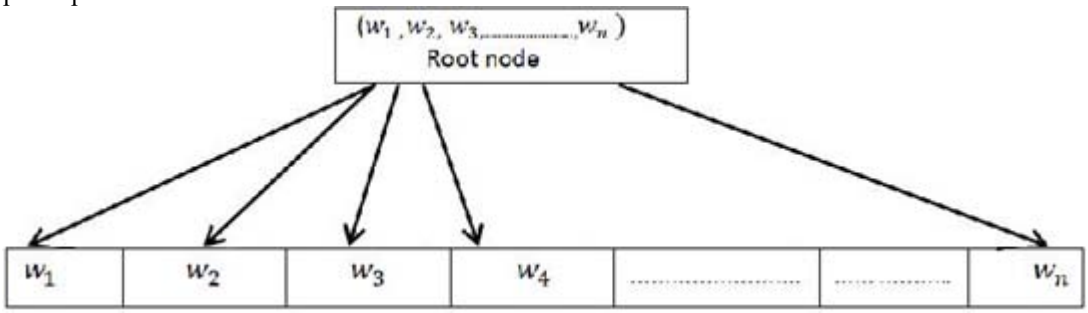

Figure 2: Root to cluster head key distribution

B. Level 2(Cluster head to cluster node connection)

This will be the wireless connected network headed by cluster head. Cluster head will distribute its key in the node using CRT based Asmuth-Bloom secret sharing scheme

A special sequence of integer used by this is known as Asmuth-bloom sequence; Here *n* is the no of nodes in a cluster and threshold is decided at*t*. This sequence must satisfy the equation

$$p_0 \prod_{i=0}^{t-2} p_{n-i} < \prod_{i=1}^{t} p_i \quad (3)$$

The dealer phase and combiner phase will be separately run in each cluster by its cluster head.

1. Dealer phase

Is selected as the secret *S* belongs to element of . The cluster node select a random no so that this value will determine that without participation of cluster head the secret key of cluster head cannot be retrieved. Secondly if value of is lower than the lower range decided for *t* threshold can be reconstructed by combining less than threshold no of shares.

Shares can be calculated by:

$$s_i = (s + \alpha p_0) mod\ p_i \quad (4)$$

2. Combiner phase

Cluster head will collect the threshold no of shares and calculate according to Chinese remainder theorem.

$$x = s_1\ mod\ p_1$$
$$x = s_2 mod\ p_2$$
$$x = s_3 mod\ p_3$$
$$\vdots$$
$$x = s_t \text{mod}\ p_t$$

Where

$$Z = p_{i_1} \cdot p_{i_2} \cdot p_{i_3} \ldots\ldots p_{i_t}$$

$$Z = p_{i_1} \cdot p_{i_2} \cdot p_{i_3} \ldots\ldots p_{i_t}$$

And value of *x* can be calculated by

$$x = \sum_{i=1}^{t} \frac{Z}{p_{i=1}} y_i s_i\ mod\ Z$$

After calculating *x* we can calculate the secret that is key for each cluster node as

$$s = x\ mod\ p_0$$

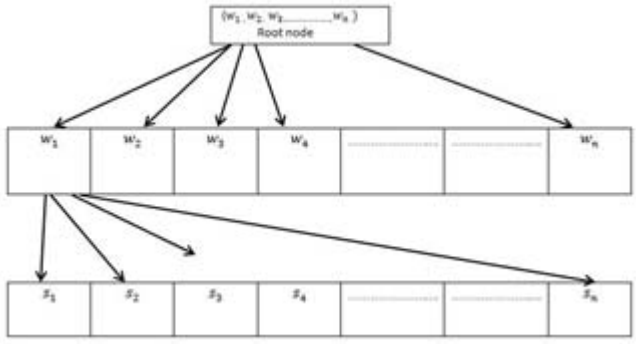

Figure 3: .key system model for given network

3. Mathematical proof

Root node to cluster head:

$$p_{n-t+2} * p_{n-t+3} * \ldots\ldots p_n < s + \alpha p_0 < p_1 * p_2 * \ldots\ldots\ldots * p_t$$

Assume that the root node have six cluster head or access point.
$^{(C}1, {}^{C}2, {}^{C}3, {}^{C}4, {}^{C}5, {}^{C}6)$
Thus root node selects six tuple series
w = (2, 3, 7, 13, 27, 53) ,

Assume *r*=11, *q*=59 and then series is calculated as = (22, 33, 18, 32, 12, 17)

and after permutation it will be

= (33, 32, 17, 18, 12, 22).

This is public key and *w* is private key series. The values of this *w* series will be distributed to the six cluster head.
Let the C1 get value 2 as share. It will distribute this value in their cluster node.

Cluster head to cluster node:

Assume that C_1 have five (n_1, *n2, n3, n4, n5*) nodes and threshold is defined as four nodes.

Dealer phase:

Secret *S*=2, cluster head choose P_0 = 3, and rest Asmuth bloom series P1 = 5, P_2 =7, P_3 =11 ,P_4 =13, P_5 =17.It satisfy the condition as;

3*13*17 < 5*7*11*13

Which give threshold range =(663, 5005). Now choosing as 663 *S*+ P_0 5005. Let = 359. *S*+ P_0=1079. Now calculating share for each node the values come as S_1 =4, S_2=1, S_3=1,S_4=9, S_5=8.

Combiner phase:

Threshold is four so let select the secret values S_1=4, S_2=1, S_3=1,*S* =9.thn the equation will be:
x=4 *mod* 5 *x*=1 *mod* 7 *x*=1 *mod* 11 *x*=9 *mod* 13

Then calculating *Z* as
Z= (5*7*11*13)

Calculating *x* by
x= (1*4*1001+1*1*715+3*1*455+5*9*385) *mod* 5005
= 23409 *mod* 5005
= 3389

Again secret can be calculated by
S = *x mod* P_0
= 3389 *mod* 3
= 2

Similarly, the entire shared secret will be retrieved by cluster head if their threshold no of participant agrees for the reconstruction. And combining all the shares from cluster

node private key can be used.

4. Security Analysis

Here we discuss the security of proposed architecture. Proposed architecture will be taken as secure, if it satisfies following properties:

Man in middle attack: This is an active attack. Here if anattacker gets the secret share of any node, then also it will not be able to compute the secret values. Because to compute the secret, attacker will need the shares of other nodes to. If, anyhow attacker manages to get the value of other secrets, then also he will need Asmuth number series to calculate the secret. This will be only known to its cluster head.

Node compromise attack: In this attack, attacker knows theprivate key of affected node. If node gets access to private key of any node then also it will not affect this architecture as they cannot access the shares of other node or other cluster.

Replay attack: This considers capture of data and itssubsequent retransmission. Any malicious and unauthorized user can repeatedly send the data which is already used. This architecture resist this replay attack as after each valid session time the value of will change. Changing the value of will change the share of each node.

Impersonation attack: here attacker pretends to be someoneelse and send the data to get the person in trouble. This architecture resists this type of attack as if any node sends the malicious data other than secret shares it will fail to calculate secret key.

5. Conclusion

In this paper two tier access structures for authentication is viewed. It is a combination of knapsack public key cryptography and Asmuth-Bloom secret sharing scheme which is unconditionally secure. Here, the architecture is combination of wire and wireless network. The unique feature of this architecture is that the collection of cluster head will work as a panel for authentication. The threshold value retrieved by combination of cluster node will work as voting result within cluster.

References

[1] Shamir A., ”How to share a secret”, Communication of the ACM, vol. 22(11), pp. 612-613, 1979.
[2] Blakley G., ”Safeguarding cryptographic keys[C]”, Proc AFIPS 1979 Natl Conf. New York:AFIPS Press 1979, pp. 313-317,1979.
[3] Gustavs J. Simmon, ”How to (really) share a secret to appear in Advance in Cryptology”, CRYPTO88.
[4] E.F Brickell, ”Some ideal secret sharing scheme”, J.Combin.Math and Combin.Comput., Vol. 9 , pp. 105-113, 1989.
[5] Deng H. Mukherjee ,AgarwalD.P.,”Threshold and Identity-based Key Management authentication for wireless adhoc network”, Information Technnology Coding and Computing Proceeding ITCC , IEEE Intern ational Conference , pp. 107-111, 2004.
[6] S.Iftene, ”General secret sharing based on Chinese remainder Theorem ”, Computer Science section 186, pp. 67-84, 2007.
[7] Azer M.A, El-Kassa S.M, El-Soudani MS. .”Threshold cryptography and Authentication in adhoc network survey and challenges”, System and Network communications, IEEE Second International conference , pp.5, 2007.
[8] Oriolfarras, CarlesPadro , ”Ideal Hierarchical secret sharing scheme”, IEEE Transaction on Information Theory, vol. 58(5), pp. 3273-3286, May 2012.
[9] L.Harh, M.foyou , ”Multilevel threshold secret sharing based on Chinese remainder theorem”. Information processing letters, vol. 114, pp. 504 - 509, 2014.
[10]Had J. Garib, KamelBlloulata , ”Authentication architecture using Threshold cryptography in Kerberos for mobile adhoc network”, Advance Science and technology Research Journal, vol. 8, No. 22, pp. 12-18, June 2014.

Author Profile

Mr. K. Balaji received the B.E. (Electronics & Communication Engineering) degree from Anna University, Main Campus, Tiruchirappalli and M.E. (Control & Instrumentation Engineering) degree from College of Engineering , Guindy. Presently he is working as an Assistant Professor in Department of Electronics & Communication Engineering at Mailam Engineering College, Mailam. His major research focuses on the cognitive acoustic networks and underwateracoustic network cross-layer design.

R. Prasanna received the B.E (ECE) degree from the V.R.S. College of Engineering and Technology, Arasur in 2008 and M.E from the G.K.M College of Engineering and Technology, Perungulathur, India, in 2011. As my research interests include Communication Engineering, Ad hoc Networks, Design issues includes OFDM MIMO and noise Suppression in MAI Systems, ASIC design, Control systems, Fuzzy logic and Networks, AI, Sensor Networks.