International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.4, April 2015 DOI:10.15693/ijaist/2015.v4i2.253-257

Enhance the Inter Cluster Communication Using CP-APE For Multicast Security In MANET

Ms.Soniya Gandhi.M
P.G student of ECE department
P.S.R.R College of Engineering For Women,Sivakasi(TN),India

Mrs.Lingadevi.K
Assistant Professor of ECE department
P.S.R.R College of Engineering For Women,Sivakasi(TN),India

Dr.k.Ramasamy
Principal
P.S.R.R College of Engineering For Women,Sivakasi(TN),India

Abstract—In order to improve the multicast security focus the cluster communication further to enhance the security rekeying mechanism is involved. In order to achieve the scalability and reliability cluster communication is the important factor .in MANET nodes have the mobility due to concern of battery power. All cryptographic techniques will be not effective if the key management is weak. The purpose of rekeying management is to provide secure procedures for handling cryptographic keying materials. Centralize approach based rekeying management scheme with group management. The network lifetime is deduced based on the energy level of nodes. Multicast key distribution in MANET have efficient clustering scheme. This scheme divides the multicast group in to cluster based on the mobility and localization of the network. in this paper we proposes the cipher text attribute based encryption attributes are attached to the user's secret key and access policy is attached to the cipher text. If attributes in the secret key of a user satisfy the policy then only the genuine user can decrypt the cipher text.

index terms— cipher text attribute based encryption, rekeying

I.INTRODUCTION

Multicast is the delivery of a message or information to a group of destination Such applications need a secure group key to communicate their data. This brings importance to key distribution techniques. In a secure multicast communication system in order to preserve the secrecy of eligible members, the key must be changed and redistributed to all the current members when some member leaves or join this group. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic.

A.Key management

Key management is a basic part of any secure communication. Key distribution and key agreement over an insecure channel are at high risk and suffer from potential attacks. Key management includes creating, distributing and updating the keys then it constitutes a basic block for secure multicastcommunication applications. Group confidentiality requires that only valid users could decrypt the multicast data.

B.Centralized key management

The centralized architectures use only one server. This server is responsible for the generation, the distribution and the renewal of the group key. A single entity is employed for controlling the whole group; hence a group key management minimize computational power on both client and server sides, and bandwidth utilization.

C.Cluster formation

Clustering focuses on dividing the networks into clusters and to choose a node as a Cluster Head. The cluster head act as the backbone of the network. But the Cluster Head selection is an important criterion because the Cluster Head will be the responsible for nodes in Clustered architecture. Each cluster group will have a specific node elected as cluster head (CH).The Head node may be selected based on a specific metric or a combination of some metric. Electing a specific node as a head node is not an easiest task.

Depending on different factors such as geographical location of the node, stability, mobility of the node, energy, capacity and throughput of the node, trusted nodes etc. The cluster head plays the role of a coordinator within its substructure. Each CH acts as a temporary base station within its cluster and communicates with other CHs. The responsibility of cluster head is to maintain the communication within the cluster and with other CH. The CH distributes the secret keys to all members' nodes inside the cluster.

Based on the secret key the data packets are shared by the nodes.If the cluster head have less energy due to the period of communication. The cluster head selection process is again revoked. Based on the less mobility and energy concern the cluster head is elected and inform the member nodes to communicated through the CH.

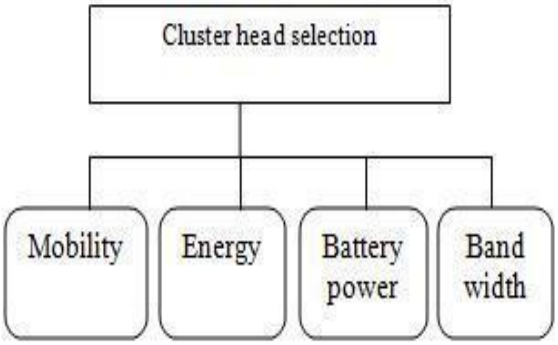

Figure 1.cluster head selection process

II.RELATED WORK

BALADE divide the multicast group in to clusters. Each cluster having the individual local controller (LC). Local controller is responsible for maintaining the individual clusters. Global controller (GC) is the source of multicast group performs the key distribution to its LC. The LC maintains the locality of group members. To maintain the integrity and confidentiality there are two types of keys are used for security purpose KEK for encryption and TEK for decryption. The computation cost is high. Due to the mobility of nodes local controller need to maintain the sustainability. Due to the maintenance of only one global controller difficult to maintain the source availability due to battery constraint.

A.SEGK

In SEGK, the common group key is generated for all nodes that common group key is shared by each members, The group key need to update in a timely fashion if there is change in group. The updating of the group key helps to enforce backward and forward secrecy of group communications. Obviously, efficiently exchanging keying materials is critical in MANETs. In SEGK, all keying materials are disseminated through the underlying multicast tree links. Due to the tree structure the link break occur the tree need to be reconstructed. Due to the factor of tree structure efficiency and reliability is high. But the delay and packet drop is increased.

Lowest ID Clustering Algorithm each node is assigned with a unique ID and it can be used to identify the malicious and friendly nodes in the network. According to lowest ID clustering algorithm, each node broadcast their own ID within the cluster after the reception of node id of neighbour nodes compare with the own id and select the lowest ID from the collection of neighbour nodes along with own id chosen as cluster head for that cluster and other nodes works as cluster members . Here, it is assumed that each CH has high backbone bandwidth and larger amount of power available with compare to other cluster members. Due to lowest id as the CH network overhead is high.

The Highest Degree Clustering Algorithm This algorithm has been developed in order to minimize the number of clusters and increase the number of nodes in each cluster. Based on the number of nodes inside the cluster the degree of nodes is high. By choosing the nodes with more connectivity with other nodes is chosen as cluster head. In contrast, it will increase traffic at each node and it will delay the transmission of packet from source to destination. Higher degree of connectivity also increases the number of collision which reduces the efficiency of the whole network and packet forwarding.

Weighted Clustering Algorithm Weighted clustering algorithm consider the degree of connectivity for each node and consider the four factors such as available battery life, transmission power, mobility. Compare the four factors with each node. The cluster head is chosen based on the nodes contain the most factors for the whole cluster and takes the responsibility to handle whole network and detect malicious nodes for security concern. In this algorithm, nodes have to update their power and battery life with all other nodes in the network and it will increase more traffic and waste of memory resources.

Mobility Based Clustering Lowest Relative Mobility Clustering Algorithm is based on the LCA algorithm but involves the relative mobility of nodes as a criterion in the cluster head selection. This mechanism reduces the CHs maintenance. However, the limitations of LCC algorithm are not completely eliminated. A novel clusters algorithm which guarantees longer lifetime of the clustering structure. The main idea is to estimate the nodes with lowest mobility chosen as cluster head. This algorithm creates clusters highly resistant to node mobility. The node with the highest weight among its neighbours is declared as the CH. This algorithm eliminates the problem of frequently changing CH due to node mobility, by allowing a node to become a CH or to join a new cluster without starting a re-clustering phase.

III.EXISTING METHOD

A.ICCR

In rekeying the centralized key manager is responsible for generate the keys to the cluster head the cluster head is responsible for generation and distribution of secret keys to the member nodes. The key generation is based on the one way function chain and shuffle algorithm.

If there is any change in the group membership, the group controller has to renew the intra-group key for the sake of forward/backward secrecy.

Forward secrecy: If a person has left a group, the departed member cannot decrypt encrypted messages transmitted after the leaving.

Backward secrecy: If a person joins a group, he cannot decrypt encrypted messages transmitted before the joining.

A one-way function is a mathematical function that is significantly easier to compute in one direction (the forward direction) than in the opposite direction (the inverse direction).It might be possible, for example, to compute the

function in the forward direction in seconds but to compute its inverse could take months or years, if at all possible.

Informally, a function f is a one-way function if

1. The description of f is publicly known and does not require any secret information for its operation.

2. Given x, it is easy to compute f(x).

3. Given y, in the range of f, it is hard to find x such that f(x) = y. More precisely, any efficient algorithm solving a P-problem succeeds in inverting f with negligible probability.

The cluster head generate the keys using the pre distributed keys further to improve the multicast security the shuffle algorithm is implemented in order to distribute the keys randomly to the member nodes inside the cluster

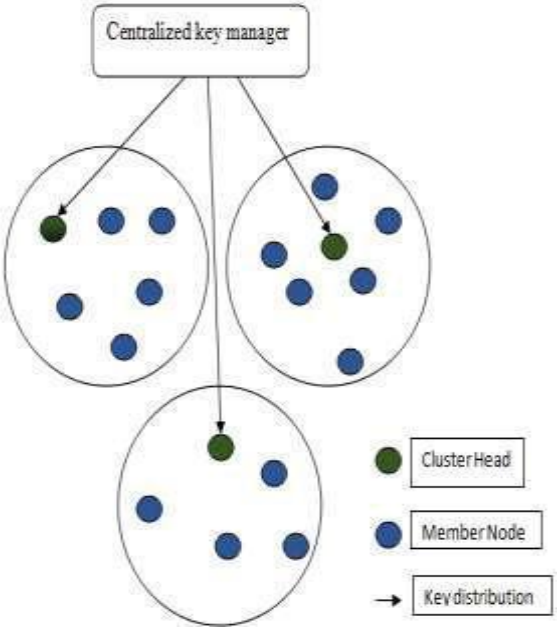

Figure 2.cluster formation and communication

IV. PROPOSED METHOD

A.Cipher text attribute based encryption

In order to improve the multicast security and to reduce the energy consumption, improve the life time of the network, reduce the mobility of nodes CP-ABE approach is efficient. Private keys have "attributes" or labels, Cipher texts have decryption policies.

In Cipher text-Policy Attribute Based Encryption (CP-ABE), each node have individual attributes. The secret key and access policy is attached to nodes for secure communication. If attributes in the secret key of a user satisfy the policy then only the authority user can decrypt the cipher text.

It keeps the encrypted data as a confidential one. it resists against the collision resistant. When a party encrypts a message in our system, they specify an associated access structure over attributes. A user will only be able to decrypt a cipher- text if that user's attributes pass through the cipher-text's access structure.

Access structures in our system are described by a mono- tonic "access tree", where nodes of the access structure are composed of threshold gates and the leaves describe attributes. We note that AND gates can be constructed as n-of-n threshold gates and OR gates.

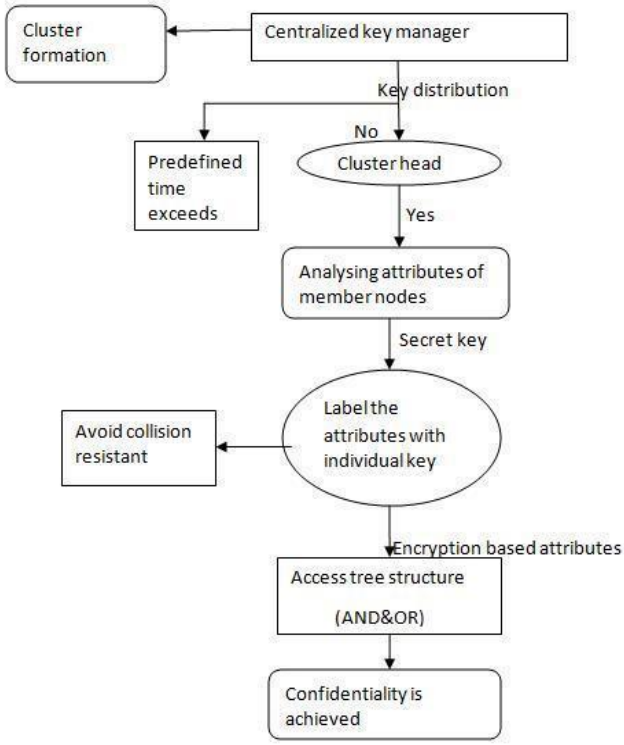

Figure 3.cipher text attribute based encryption process

Scenario: 1

Packet delivery ratio:It is the ratio of number of packets received and total number of packets transmitted.

Scenario: 2

Energy consumption: it is the amount of energy consumed for total communication process

Scenario: 3

Security cost: it is the number of keys updated over total keys.

Scenario: 4

Resilience against node capture:it is calculated between non compromised nodes by a capture of x-nodes

Our simulation settings and parameters are summarized in table 1.

No. of Nodes	50
Area Size	1500 X 300
Mac	802.11
RadioRange	120m
Simulation Time	910 sec
Transmission power	0.660
Packet Size	256bytes
Mobility Model	Random Way Point

V .RESULT

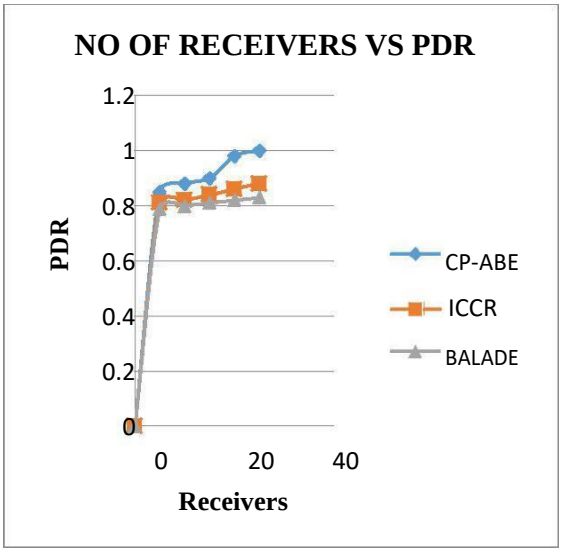

Figure 4. Receivers against PDR

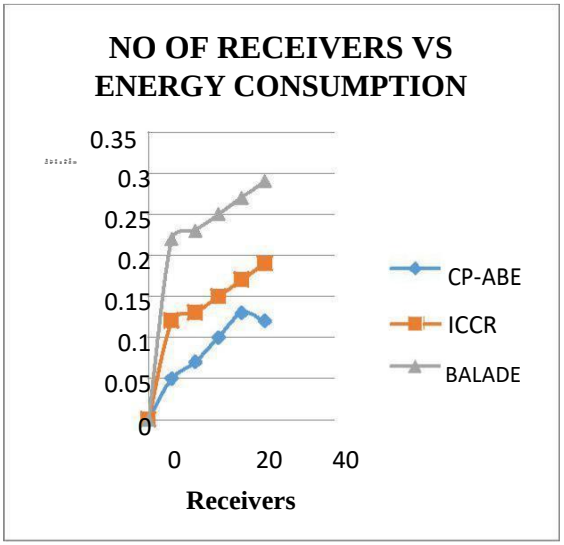

Figure 5. Receivers against energy consumption

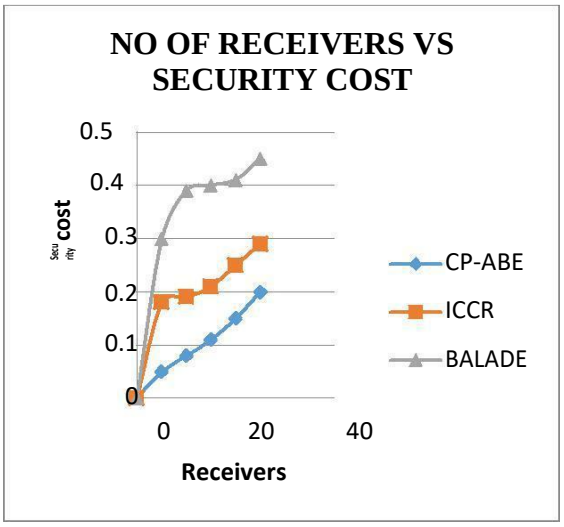

Figure 6. Receivers against security cost

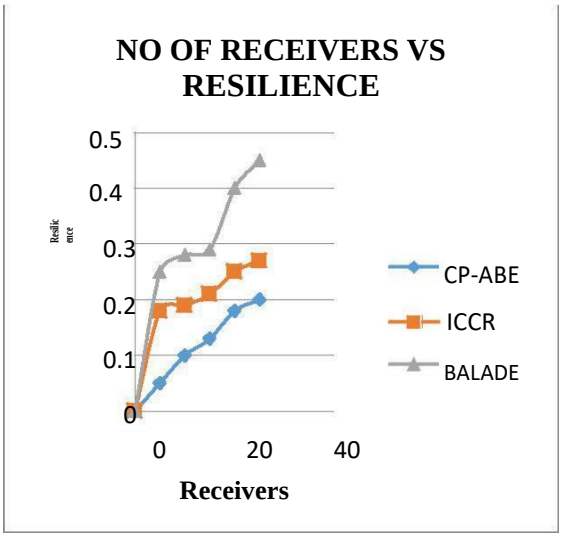

Figure 7. Receivers against resilience

VI. CONCLUSION & FUTURE WORK

In this paper we proposed CP-ABE over the schemes BALADE,ICCR reduce the security cost provide resistant against more security attacks and the packet delivery ratio is improved up to 50%.the energy consumption is reduced due to the CP-ABE but in ICCR the rekeying is needed during every node joining and leaving the cluster.

REFERENCES

[1] Vennila, rajamanicam, duraisamyveerapan"intercluster communication and rekeying technique for multicast security in MANET" IEEE the institute of engineering and technology 2014.

[2] A.Rekha, P.Anitha, A.S.Subaira, C.Vinothini "A survey on encryption algorithms for data security" IJRET: International Journal of Research in Engineering and Technology,2014.

[3] Yao Yu+, Lincong Zhang "A Secure Clustering Algorithm in Mobile Ad Hoc Networks" IPCSIT vol. 29 (2012).

[4] Mohammad Shayesteh and NimaKarimi, Member, IACSIT," An Innovative Clustering Algorithm for MANETs Based on Cluster Stability", International Journal of Modeling and Optimization, Vol. 2, No. 3, June 2012 .

[5] LeinHarn and ChangluLin , "Authenticated Group Key Transfer Protocol Based on Secret Sharing", IEEE transactions on computers, vol. 59, no. 6, June 2010.

[6] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Mediated ciphertext-policy attribute-based encryption and its application," in Proc. WISA, 2009, LNCS 5932, pp. 309–323.

[7] Mohamed M. NasreldinRasslan, Yasser H. Dakroury, and Heba K. Aslan "A New Secure Multicast Key Distribution Protocol Using Combinatorial Boolean Approach" ,International Journal of Network Security, Vol.8, No.1,
PP.75–89, Jan. 2009.

[8] S. Benson Edwin Raj, J. JeffneilLalith , "A Novel Approach for Computation-Efficient Rekeying for Multicast Key Distribution" IJCSNS , VOL.9 No.3, March 2009.

[9] RatishAgarwal, Dr. Mahesh Motwani, "Survey of clustering algorithms for MANET". International Journal on Computer Science and Engineering Vol.1 (2), 2009,98-104 .

[10] Bing Wu, Jie Wu" An efficient group key management scheme for mobile ad hoc networks", Int.J.SecurityandNetworks,Vol 2008.

[11] LihaoXu, Cheng Huang, "Computation Efficient Multicast Key Distribution," IEEE Trans. Parallel And Distributed Systems, Vol 19, No. 5, May 2008.

[12] D.Huang, D.Medhi, A Secure Group Key Management scheme for Hierarchical Mobile Adhoc Networks, Adhoc Networks, June 2008.

[13] M. Bouassida, I. Chrisment, and O. Festor: Efficient Group Key Management Protocol in MANETs using the Multipoint Relaying Technique. International Conference on Mobile Communications 2006.

[14] Sencun Zhu† SanjeevSetia‡ ShouhuaiXu§ SushilJajodia "GKMPAN: An Efficient Group Rekeying Scheme for Secure Multicast in Ad-Hoc Networks" IEEE first Annu. Int. conf on mobile and ubiquitous Systems:Networking and services 2004.

[15] T. Chiang and Y. Huang. Group keys and the multicast security in ad hoc networks. In Proceedings of the International Conference on Parallel Processing Workshops, 2003.

[16] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz. Secure multicast groups on ad hoc networks. In Proceedings of the 1st ACM workshop on security of ad hoc and sensor networks, pages 94–102. ACM Press, 2003.

[17] Chung KeiWong, Mohamed Gouda, and Simon S. Lam. Secure group communications using key graphs. IEEE/ACM Trans.2000.