Secure group communication over MANET using hybrid Key Management

S.Fiona abishag, Dr.P.Deepalakshmi

Abstract— In many newly emerging network there is a need to provide secure transmission within the network.MANET is one such network which requires secure group communication.The key concept in security is key management.In the existing key management systems third party is fully trusted for key generation.Hence the trustworthiness of third party is more important to provide secure communication.Here we propose a hybrid approach which combines group key agreement and broadcast based encryption techniques.The major advantage is that it avoids the need to rely fully on a trusted third party.Here we use a provable secure protocol which provides resistance against blackhole attack such that secure and efficient routes will be provided to reach the destination.Thus the new paradigm facilitates a fast and secure transmission to remote groups.

Index Terms— MANET,Key management,Information security,Adhoc networks,Group key agreement,Broadcast based encryption,Blackhole attack.

1 INTRODUCTION

A Mobile Adhoc Network(MANET) is an autonomous system of mobile routers connected by wireless links the union of which form an arbitrary graph.The routers are free to move randomly and organize themselves arbitrarily and hence the networks topology may change unpredictably.Due to the lack of infrastructure support,each node acts as a router and forwards data packets to other nodes.

MANETs can be classified into three major categories as Vehicular adhoc networks(VANET),Internet based mobile adhoc networks(iMANET),Intelligent Vehicular adhoc networks(InVANET) ,each having a specific purpose. As there are many advantages in MANET it can be applied in several areas such as military battle field, commercial sector,personal area network,one to many data dissemination,video conferencing and so on.

Key management is the key concept in MANET.Key management refers to the management of cryptographic keys in a cryptosystem which includes dealing with the generation,exchange,storage,use, distribution and replacement of keys. The major challenge in MANET is to maintain security in group communication. Many key management schemes were proposed previously which still proves to be insecure.In the present schemes,third party is fully trusted and the process of key generation and distribution takes place through the third party across the insecure network.In our scheme we propose a new key management technique which overcomes all the defects and enhances security and secure protocol to provide resistance against blackhole attack

2 RELATED WORK

Key management is the major security concern in group oriented communication.In MANET it is important to support group oriented communication such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios and so on.It is a challenging task to maintain security in group communication over MANET since the risk of unsecured sensitive information being intercepted by unintended recipients is the real concern.In the existing system key management is classified into two groups as Group key agreement and Key distribution system.At present these are the two major research areas.The first approach is group key agreement in which a group of users negotiate the secret key via open insecure network. All users share the same secret key to encrypt/decrypt messages. It proves to be secure for intra group communication as it does not require a centralized key server to generate and distribute secret keys to all users .But in this approach the secret key travels through the network and hence there is a lot of possibility to hack the secret key and thereby all the information can be hacked.Group key agreement is more prune to attacks and hence insecure. The earlier approaches provide effective member join but in case of member leave it is comparitively high .Tree structure has been followed which provides efficient member join/leave and the analysis shows that the lower bound for worst case cost is O(log n) where n is the number of group members.

In key distribution system a centralized server allocates the secret key to all users such that only the intended recipients can read the transmitted message.Member addition/deletion is not supported by early key distribution protocol.Broadcast encryption is the approach in which the senders can freely choose the intended recipients to form the initial group.The Broadcast encryption scheme can be classified into two categories as symmetric key broadcast encryption and public key broadcast encryption. In symmetric key scheme the central key server generates secret keys and broadcasts messages to users and hence only the key generation center can be the sender.In public key setting the centralized key server generates public key in addition to the secret key for all users so that anyone can play the role of sender.This scheme limits the number of receivers and only N receivers can receive the transmitted message.

Inorder to maintain secure communication it is important to provide resistance against attacks.MAODV protocols are used for route discovery in group communication.In route discovery phase each node sends the RREQ message and waits for the RREP message from other nodes to obtain the route to reach the destination.The freshness of route is identified by the sequence number (ie)sender chooses the path with the highest sequence number.Black hole is an attack in which the malicious node blocks the route to reach the destination by sending highest sequence number .So many research analysis have proved that security is breached easily in the existing protocol.

3 MOTIVATION

The existing key management system lacks security since the third party is fully trusted for secret key generation and distribution.If the centralized server is hacked then security can be breached easily.Also the key distribution process happens through the insecure network.Security is under high risk in the exiting system.The member join/leave is also much expensive and inefficient.The system limits the number of receivers and also the senders need to be static.The system fails to provide security against attacks such that data confidentiality,integrity,availability cannot be maintained.

4 HYBRID KEY MANAGEMENT TECHNIQUE

A new key management technique is proposed which is the combination of group key agreement and broadcast based encryption.In this hybrid approach each user generates a public,private key pair.The users registers their public key to the centralized authority and keeps the private key secret.A remote sender who wishes to send messages will retrieve the public keys of receivers and check their authenticity before sending messages. After that the sender communicates with the group of receivers.The major criteria of this key management approach is to securely distribute the secret key to the intended receiver group and here it is done using an encapsulation mechanism.Secure key distribution is achieved using the algorithms specified below.

- Key generation : The key generation algorithm is run by each user u_i to generate the public/private key pair.The user takes n,N as their inputs and i as the index to generate (pk_i,sk_i) as their public,private key pair.The key generation process can be done offline before the message transmission starts online.Each user randomly chooses public key P_i which belongs to the group Z_p and generates secret key Si as

  $$S_i = g^{Pi}$$

- Encryption : The encryption algorithm is run by each sender who wishes to start communication with the group of receivers.Here a secret session key k is generated with which messages can be encrypted and sent to the receivers.Only the intended receivers can decrypt the key and hence the message.The secret session key is generated as follows.

  - ➢ Randomly select r,P_i belongs to Z_p and compute
    $S_{i0} = \ g^{Pi}, Y_{io} = (S_{i1}/S_{in})^{Pi}, c=g^r$
  - ➢ Extract the public group encryption key as
    $K = e(S_{i1},S_{i2})e(S_{i2},S_{i3}).....e(S_{in-1},S_{in})$
  - ➢ Compute
    $S = Ke(S_{in},S_{i0})e(S_{i0},S_{i1})$
  - ➢ Compute secret session key
    $k=S^r$
  - ➢ Broacast the header
    $Hdr = (S_{i0},Y_{i0},c)$

- Decryption : The Decryption algorithm is run by all the receivers inorder to decrypt the secret session key hidden in the header and thereby decrypt the message.The decryption process is as follows.

  - ➢ Each receiver Uij publishes
    $Yij = (S_{ij+1}/S_{ij-1})S_{ij}$
  - ➢ Each receiver indexed by ij can decrypt the secret session key
    $d = S_{ij-1}^{(n+1)Pij} \ Y_{ij}^{n} \ Y_{ij+1}^{n-1}.......Y_{ij-2}$
  - ➢ By using d each receiver can extract the secret session key k by computing
    $k=e(d,c)$

Thus the Key generation process with the new key management scheme is done in a secure fashion.Here only the intended receivers can decrypt the secret session key and hence it proves to be secure.

5 RESISTANCE AGAINST BLACKHOLE ATTACK

Adhoc networks are more vulnerable attacks and security in adhoc networks is under high risk.MAODV is rhe protocol widely used for group communication.The protocol is used to find routes to reach the destination and it is done using route discovery process.The node that wishes to communicate will send a RREQ message to the nearby nodes and waits for reply.If the node that receives the request contains fresh enough route to reach the destination it sends back a RREP message or otherwise forwards the request the other nodes.The freshness of route is decided with the sequence number and the node which sends reply with high sequence number is selected.The major issue here is a malicious node may send fake RREP message to the source with required parameter and assures packet delivery to destination.Once the packet transmission starts from the source,the malicious node drops all the packets without forwarding them to the destination.This may cause a serious effect in the network.Blackhole is a malicious node which drops all packets passing through them without reaching the destination.

The proposed Secure MAODV protocol provides extensive security against blackhole attack.In this protocol the RREP message from the nodes which have already routed is only considered.Any new node which sends reply with fresh routes are also discarded.Also the node which sends timed out replies are considered as malicious nodes and once the malicious node is found its id is broadcasted to all other nodes in the network so that further transmission through the malicious node can be avoided.

6 SIMULATION SETUP

The simulation is done using NS2 simulator with 50 mobile nodes with a flatgrid topology of 1500x300 area.A node is set as the sender with the group of receivers varying from 10,20.. and so on.Various analysis is performed to measure the delay,speed,packet delivery ratio,throughput and comparision between the existing and new algorithm to generate secret session key interms of security.The results shows that transmission takes place in a speed ranging 100m/s.Also the total delay in communicating within the network is less than 0.1 micro seconds.The security analysis between RSA and pairing algorithm has proved that our algorithm is more secure since it uses dynamic key generation and key encapsulation mechanism.Packet delivery ratio is above 85 percent which shows that dropping of packets is comparatively low .Our algorithm proves to provide fast and secure transmission to remote groups.

7 RESULTS AND DISCUSSION

From the simulation results pairing algorithm is considered more secure for key generation than RSA algorithm.The graph shows the security levels with number of nodes in x axis and security range in y axis.

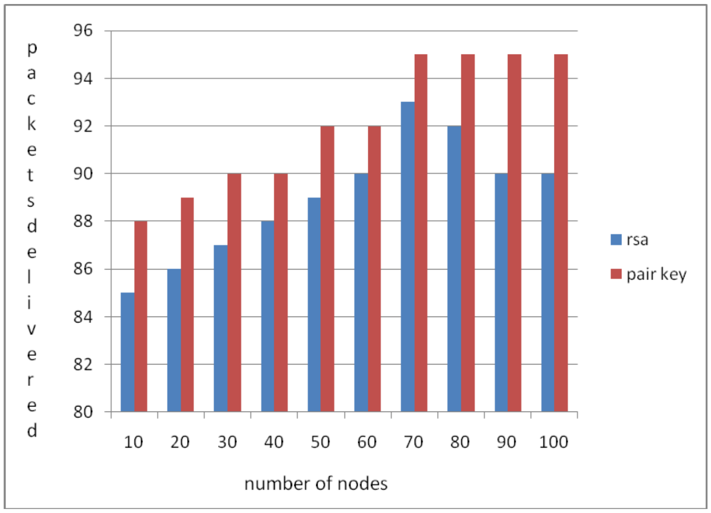

Fig 1.1 .Comparision between rsa and pair key algorithm interms of security

The above figure shows the security analysis between rsa algorithm and pairing algorithm interms of number of packets delivered successfully.It has been observed that number of packets delivered successfully is high in our algorithm. Also it is proved that pairing algorithm is more secure since it uses dynamic key generation and key encapsulation mechanism.Here one of the most important feature in our algorithm is that it does not send the secret session key directly to the receiver group,instead it sends the index with which the key is generated.There is no possibility for the intruder to acquire the key.Hence the message remain secure and can be decrypted only by the intended receivers.

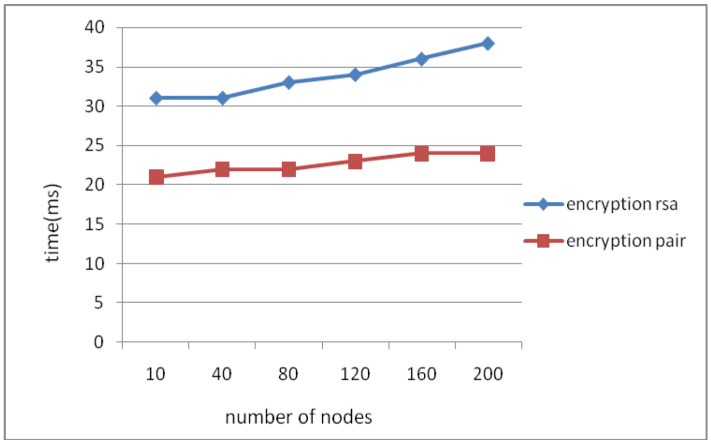

Fig 1.2.Time taken for encryption

The above figure shows time taken for encryption with number of nodes in x axis and time in y axis.The analysis shows that our algorithm allows user to encryprt messages faster than using rsa algorithm.

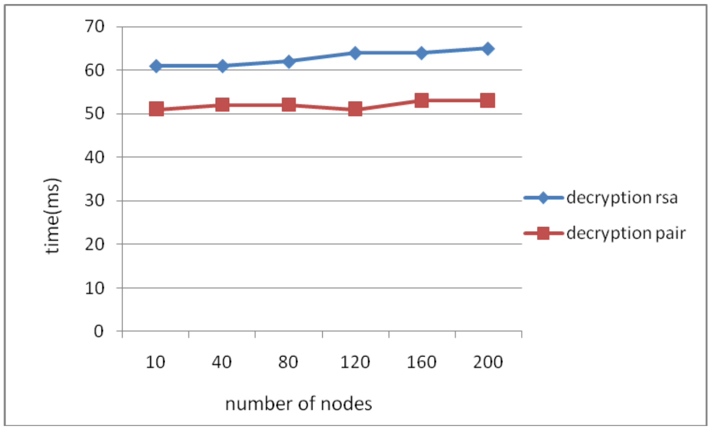

Fig 1.3.Time taken for decryption

The above figure shows time taken for decryption with number of nodes in x axis and time in y axis.The analysis shows that our algorithm allows user to decryprt messages faster than using rsa algorithm.Hence the message can be read by the receiver quickly.

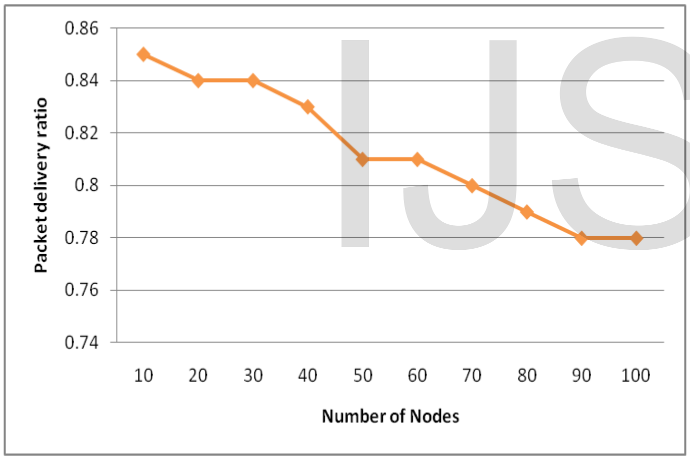

Fig 1.4.Packet delivery ratio

The above figure shows the packet delivery ratio with number of nodes in x axis and PDR in y axis.PDR refers to the ratio between the number of packets received to that of the number of packets sent.As per the analysis PDR is measured above 85 percent so the dropping of packets is comparatively very low.

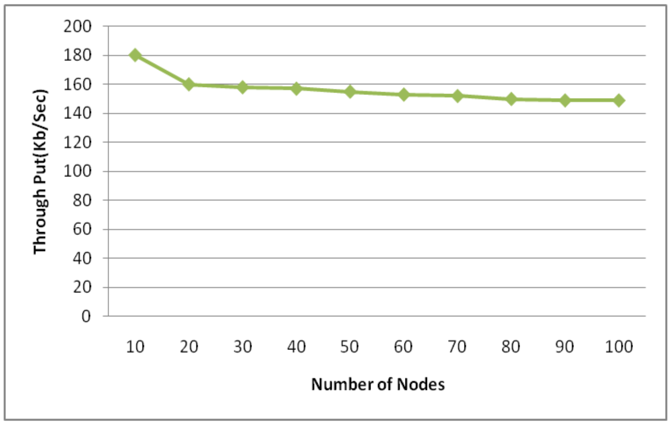

Fig 1.5.Throughput

The above figure shows the throughput with number of nodes in x axis and throughput interms of kilobytes per second in y axis.Throughput is defined as the number of packets that are successfuly delivered in a specified time.The analysis shows that throughput is high and packets are delivered successfully to the destination.Finally the results shows that our approach is provide secure transmission when compared to existing approaches.The algorithm proposed for secret session key generation in our key management approach can be used to securely transmit messages in the network.

7 CONCLUSION AND FUTURE WORK

Here we have proposed a hybrid key management approach by incorporating the ideas of group key agreement broadcast based encryption.The system proves to be secure since it does not fully rely on a centralized server.Also Key generation is done using pairing algorithm which is based on dynamic key setting and key encapsulation mechanism.The algorithm is secure since it does not require to send the secret key directly to the receiver.Inaddition to this Secure MAODV protocol is proposed inorder to provide resistance against blackhole attack.Hence end to end delivery is assured without dropping of packets.Also member join/leave is much easier compared to previous approach.This approach can be used in various realtime applications to securely transmit messages.In future this approach can be used for group communication in various other types of adhoc network.

REFERENCES

[1] Qianhong Wu, Member, IEEE, Bo Qin, Lei Zhang, Josep Domingo-Ferrer, Fellow, IEEE, Jes´us A. Manj´on, "Fast Transmission to remote cooperative group-A New Key Management Paradigm," IEEE/ACM transactions on networking , vol. 21,no. 2,Apr. 2013.

[2] Y. Zhang and Y. Fang, “ARSA: An Attack-Resilient Security Architecture for Multi-Hop Wireless Mesh Networks,” IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[3] K. Ren, S. Yu, W. Lou and Y. Zhang, “PEACE: A Novel Privacy-

Enhanced Yet Accountable Security Framework for Metropolitan Wireles Mesh Networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no.2, pp. 203-215, Feb. 2010.

[4] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu and S. Guizani, "A Pyramidal Security Model for Large -Scale Group-Oriented Computing in Mobile Ad Hoc Networks: The Key Management Study," IEEE Trans. Veh. Technol., vol. 58, no. 1, pp. 398-408, Jan. 2009.

[5] Y-M. Huang, C.-H. Yeh, T.-I. Wang and H.-C. Chao, "Constructing Secure Group Communication over Wireless Ad Hoc Networks Based on a Virtual Subnet Model," IEEE Wireless Comm., vol. 14, no. 5, pp 71-75, Oct. 2007.

[6] L. Zhang, Q. Wu, A. Solanas and J. Domingo-Ferrer, "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," IEEE Trans. Veh. Technol., vol. 59, no. 4, pp. 1606 - 1617, May 2010.

[7] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Sel. Areas Commun., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.

[8] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," in Advances in Cryptology– EUROCRYPT'94, LNCS, vol. 950, pp. 275-286, 1995.

[9] M. Waldvogel, G. Caronni, D. Sun, N. Weiler and B. Plattner, "The VersaKey Framework: Versatile Group Key Management," IEEE J. Sel. Areas Commun., vol. 17, no. 9, pp. 1614-1631, Sept. 1999.

[10] M. Steiner, G. Tsudik and M. Waidner, "Key Agreement in Dynamic Peer Groups," IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769-780, Aug. 2000.

[11] A. Sherman and D. McGrew, "Key Establishment in Large Dynamic Groups Using One-way Function Trees," IEEE Trans. Software Eng., vol. 29, no. 5, pp. 444-458, May 2003.

[12] Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, "Secure Group Communication Using Robust Contributory Key 0Agreement," IEEE Trans. Parallel Distrib. Syst., vol. 15, no. 5, pp. 468- 480, May 2004.

[13] Y. Kim, A. Perrig and G. Tsudik, "Tree-Based Group Key Agreement," ACM Trans. Inf. Syst. Security, vol. 7, no. 1, pp. 60-96, Feb. 2004.

[14] Y. Sun, W. Trappe and K.J.R. Liu, "A Scalable Multicast Key Management Scheme for Heterogeneous Wireless Networks," IEEE/ACM Trans. Netw., vol. 12, no. 4, pp. 653-666, Aug. 2004.

[15] W. Trappe, Y. Wang and K.J.R. Liu, "Resource-Aware Conference Key Establishment for Heterogeneous Networks," IEEE/ACM Trans. Netw., vol 13, no 1, pp.134-146, Feb. 2005.

[16] P. P. C. Lee, J. C. S. Lui and D. K. Y. Yau, "Distributed Collaborative Key Agreement and Authentication Protocols for Dynamic Peer Groups," IEEE/ACM Trans. Netw., vol. 14, no. 2, pp. 263-276, April 2006.

[17] Y. Mao, Y. Sun, M. Wu and K. J. R. Liu, "JET: Dynamic Join-Exit-Tree Amortization and Scheduling for Contributory Key Management," IEEE/ACM Trans. Netw., vol 14, no 5, pp.1128-1140, Oct. 2006.

[18] W. Yu, Y. Sun and K. J. R. Liu, "Optimizing the Rekeying Cost for Contributory Group Key Agreement Schemes," IEEE Trans Dependable and Secure Computing, vol. 4, no. 3, pp. 228 - 242, July-Sep. 2007.