ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A Study on Key Management in MANETs

C. Mohammed Gulzar[1], Dr.P.Nageshwar[2], S.Imran Pasha[3]

Associate Professor, Dept. of CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool, A.P., India

Assistant Professor, Department of Computer Applications, M.V.S Govt. Degree College, Mahabubnagar, India

Assistant Professor, Dept. of CSE, Dr. K.V. Subba Reddy Institute of Technology, Kurnool, A.P., India

ABSTRACT: Group key management is one of the basic building blocks in collaborative and group-oriented applications in Mobile Ad Hoc Networks (MANETs). Group key establishment involves creating and distributing a common secret for all group members. However, key management for a large and dynamic group is a difficult problem because of scalability and security. Dynamical changes in network's topology causes feeble conviction relationship among the nodes in the network. In MANETs a mobile node operates as end terminal as well as an midway router. Therefore, a multi-hop situation occurs for communication in MANETs; where in between source and destination there may be one or more malicious nodes. In this paper, we proposed a key management scheme. We assume that MANETs is alienated into groups having a group leader in each group. Group leader has accountability of key management in its group. Proposed key management scheme is a decentralized method that does not need any Trusted Third Party (TTP) for key management. In proposed key management scheme, both a new node and group leader validates each other equally before joining the network.

KEYWORDS: MANET, Group, Key management, Authentication, Secure routing.

I. INTRODUCTION

A MANET is a special type of wireless network in which mobile hosts are linked by wireless interfaces forming a temporary network without any fixed infrastructure. In MANET, nodes communicate each other by forming a multi-hop radio network. Mobile nodes operate as not only end terminal but also as an intermediate router. Data packets sent by a source node can reach to destination node via a number of hops. Thus multi-hop scenario occurs in communication and success of communication depends on nodes' cooperation.

Security of a network is a vital factor that must be considered in building the network. A network has to attain security necessities in terms of authentication, confidentiality, integrity, availability and non repudiation. These security necessities rely on the availability of secure key management system in network. Primary goal of a key management system in a network is to issue the keys to the nodes to encrypt/decrypt the messages, to manage these keys and to prevent the improper use of legally issued keys. Lack of key management system makes a network susceptible to several attacks[7]. Therefore, key management system is the basic and important need of a network for secure communication. A key management system normally involves key generation, allocation, updation and revocation of keys in network. The feature of MANETs such as dynamic topology, lack of federal authority, resource inhibited and node mobility are the major challenges in organization of key management. Some techniques such as intrusion detection mechanism devour lot of nodes' battery power but cannot report for flexible membership changes. However, a well-organized and secure key management system can solve this problem with a reasonable cost.

On the other hand, mobile ad hoc networking is multi-hop relaying, i.e. messages are forwarded by several mobile nodes from source to destination, if destination node is not directly reachable. In other words, nodes in MANET operate as not only end terminal but also as an intermediate router. Thus, multi-hop scenario occurs; where an attacker can insert, catch or modify the messages easily in absence of secure routing protocol. This means that insecure MANET is susceptible to many attacks [21] such as wormhole attack [22], black hole attack [23] including node imitation, message inoculation, loss of confidentiality etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

In this paper, we proposed a key management scheme for group based MANETs in which a group leader can generate, distribute, update and revoke keys in its group and a provable secure routing protocol. Proposed key management scheme neither depends on a central server nor is it fully dispersed. Our key management system forms a decentralized system that combines both centralized key management as well as disseminated key management so that it can unite merits of both methods. Proposed key management scheme is a mixture key management scheme that uses both Symmetric Key Cryptography (SKC) for secure communication and Public Key Cryptography (PKC) to authenticate other nodes and to share a session key.

Rest of the paper is organized as follows. In section 2, grouping and algorithm to elect group leader is discussed. Key management system is proposed in section 3. Security analysis of proposed key management system is discussed in section 5 and finally, section 6 gives conclusions.

II. GROUP INFORMATION

Grouping or clustering is a process that divides the network into interconnected substructure known as groups. Grouping provides a better solution to the problem of key management and routing in MANET. There is a group leader as coordinator in every group. Each group leader acts as a temporary base station within its zone or group and communicates with other group leader. A system model of open MANET is shown in Figure.1. Mobile nodes are divided into several groups in such a way that all the nodes are roofed with no groups overlapped. Some of the nodes are selected as group leaders to perform the functions of key management system and other administrative functions in its group. Aim of constructing the grouped based structure is that grouping preserves the structure of network as long as possible, when nodes moves or topology is slowly changing. On the other hand, grouping reduces the number of keys required to give out in network for secure communication.

Group based structure distributes the functions of a central server into several nodes (group leaders). Therefore, it combines both centralized and distributed approaches of key management system providing a decentralized solution. Group based structure of networks also removes the vulnerability of compromising single central server. If a group leader is compromised; only a group will be compromised leaving rest of the network safe and secure.

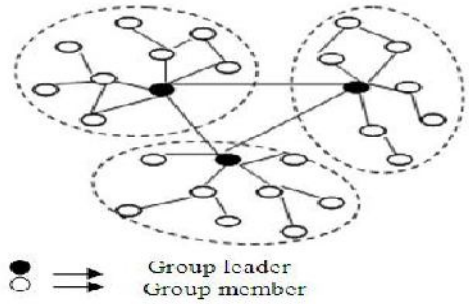

Figure 1. System model for MANET

Algorithm: Electing Group Leader in a Group

A good grouping algorithm is one that divides the network into groups in such a way that it preserves the structure of network as long as possible and fast recovery from fault such as electing new group leader on the failure of existing group leader.

To select a well suited group leader, we take into account of its mobility, battery power and behavior of node. The following features are considered for grouping:

• Each group leader is able to support maximum ‘x’ number of nodes (a pre-defined value) efficiently. If a group leader is trying to serve more than ‘x’ nodes, system’s efficiency suffers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

• 'Mobility' is the significant aspect in deciding the group leader. Group leaders are in charge to conserve the structure of group as much as possible when nodes move. Moving group leader rapidly results detachment of nodes from group leader and also increases the probability of nodes' compromised. Mobility of a node is indicated by 'M' and can be measured as:

$$M = \frac{1}{T}\sum_{t=1}^{T}\sqrt{(Xt - Xt-1)^2 + (Yt - Yt-1)^2}$$

Where, (Xt, Yt) and (Xt-1, Yt-1) are the coordinates of a node at time t and t-1.

• 'Battery power' (B) is another significant factor to decide a group leader. A group leader consumes more battery power than a normal node because a group leader has further responsibilities such as monitoring group members and allocation of keys in the group. Therefore, a node should be elected as group leader with maximum battery power.
• Another important constraint for electing the group leader is the 'behavior of node'. Security of a group is entirely relies on group leader. Group Leader monitors the nodes' behavior continuously in the group and assigns them a Trust Level (T).

Finally, group leader is selected on the basis of weight (W), is defined as:

$W = W_0M + W_1B + W_2T$
where, W_0, W_1, and W_2 are the weight factor such as:
$W_0 + W_1 + W_2 = 1$

Choose a node as group leader with the least weight (W).

III.PROPOSED KEY MANAGEMENT SCHEME

In this section, we proposed key management system for group based MANETs. Proposed key management scheme includes key generation, distribution and revocation phase. We formulate following assumptions:

• An offline Trusted Third Party (TTP) is obtainable outside the network which is accountable only to issue a certificate and public/private key pair for mobile nodes.
• Intergroup communication is done through group leaders.
• Group leaders are trusted. Grouping algorithm is not periodic. This reduces updates and hence computation and communication cost in system.

Key Generation and Distribution
All group leaders in network are assigned a unique id. Each group leader has a public/private key pair and a secure hash function (for e.g. SHA or MD5). We classify three types of keys in the network: Group key, key for all the members in group used to encrypt/decrypt all the traffic communicated in the group. Second key, a symmetric key shared between group leader and a member node of same group and third key, shared by all group leaders in network.

Group leaders generate group key for their groups separately. Group key is updated each time when a node joins or leaves the group to maintain the forward and backward secrecy. Second key(k) is shared between group leader and a member node at the time when node joins group. k is the function of node_id and a secret arbitrarily generated number by group leader.

$$f(node\_id, N) = k$$

where f is a secure hash function selected by group leader , node_id is assigned to a node at the time of joining and N is a secret number known only to group leader.

Third key is shared by group leaders in network. Group leaders can agree on a key to communicate securely using Group Diffie-Hellman key agreement protocol [15]. Key is updated when group leader election algorithm is raised in any group; new elected group leader can start Group Diffie-Hellman key agreement to update the key.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Node addition

Whenever, a new node joins a group, it sends a request to group leader. This request might be captured by a malicious node viewing as group leader to new node. Similarly, a malicious node can also send a request to group leader to connect the group. Therefore, it is necessary for both group leader as well as new node to verify each other. Upon successfully mutual verification, a node can join the group and share a key with group leader in a secure way. A new node and group leader can validate each other using challenge-response protocol. New node sends a challenge to group leader and group leader provides an applicable response to prove its novelty.

Group leader selects two large prime numbers 'p' and 'q' and computes: N=p*q, then selects an arbitrary secret number 'S' and computes=S2 mod N (1<S<N).

'N' and 'V' are openly available in the group. When group leader has to verify itself i.e. it received a challenge from a node, it finds X=R2 mod N, where 'R' is a random number selected by group leader such that 1<R<N.

Group leader sends {N, V, X} to new node. On receiving (N, V, X), new node sends a challenge 'c' to group leader. Group leader calculates Y=RSC mod N and send it to node. Node calculates XVC and contest with Y2. If both values are same, group leader is successfully validated.

After successful validation of group leader, new node can sends its certificate to group leader issued by offline TTP. Group leader verifies nodes' certificate, and extracts the public key of node from certificate. Group leader generates a node_id and sends node_id and a key generated by function f shared by group leader and node, encrypted with public key of new node. Group leader then modernize group key and group members list and sends to the members of group. Communication between group leader and new node takes place as follows:

A group of mobile nodes with a group leader of MANET is shown in Figure.2, where a new node 'A' wants to connect the group. Following are the notations used in communication:

G→ Group, {L, M}
M→ Set of group members {m1, m2, m3 …mn}
L→ Group leader
A→ New node
ID_A→ A's Identity given by group leader
K_{XY}→ Session key shared between node X and Y
e_x/d_x→Public key/Private key of node X
DS_X→ Digital Signature of node X
T_X→ Timestamp added by node X
$CERT_X$→ Certificate of node X
S_{LX} Symmetric key shared between group leader and node X.
X: Y {k(M)} Node X sends a message M encrypted with key k to node Y

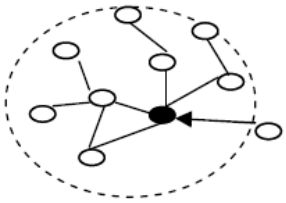

Figure 2. A Group in MANET

A : L {A, Join_req}
L : A U M {N, V, X}
A : L U M {c}
L : A U M {Y}

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

A : L {$CERT_A$}
L : A {e_A (e_L, ID_A, SL_A)}
A : L {SL_A (num}
L : A {SL_A (num, member_list, group key)}
L : M {group_key (new_group_key)}

Key Agreement Protocol

If a node A wishes to communicate securely with node B. They must agree on a session key before starting communication. Communication begins when A sends message:

A : B {e_B (ID_A, ID_B, T_A, DS_A)}

On receiving message from A, B decrypts the message and verifies the signature of A by public key of A. If node B does not have A's public key, it sends a message to group leader conveying to send A's public key. Here following two cases are possible:

• A is a genuine node and group leader has pubic key of A. In this case, group leader sends A's public key to B. B then verifies A's signature and share a session key K_{AB}.

B : A {e_A (ID_A, ID_B, T_A, T_B, DS_B)}
A : B {e_B (T_A, T_B, num1, K_{AB})}
B : A {K_{AB} (num1, num2)}

• In second case, A is malicious node and not a member of group. In that case, group leader would inform to all the member of group about node A.

Node Deletion

Nodes in a group communicate with group leader occasionally showing its attendance in group. If a node doesn't communicate, group leader removes that node from member list and inform other members. Group leader regenerates new group key and sends other nodes in group, encrypted by their public key. A node can be removed from member list when one of the following events occurs:

• A node can leave the group with prior notification.
• A node can leave the group without any prior notification or node is not forwarding the messages or acting as malicious node. Group leader eliminate that node vigorously. In this case, group leader must notify to neighbor leader nodes.
On the other hand, a new group leader must be elected that can direct the group whenever a group leader leave the group with or without prior notification. New group leader reconstructs new group key and distributes in the group encrypted with the public key of members and share a new symmetric key with each member in group. New group leader shares its public key and id to other group leader in network and starts Group Diffie-Hellman key agreement [13] to update key shared by group leaders.

IV.SECURITY ANALYSIS OF PROPOSED SOLUTION

In this section, we discussed the security analysis of proposed key management system against different attacks.

Key Management Scheme

Backward Secrecy
When a node leaves the network, it should not be able decrypt the future encrypted traffic. In proposed key management scheme, whenever a node leaves the group, group leader regenerates new group key and distribute it in the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

group. On the other hand, when a group leader leaves the network, a new group leader generates group key for the group. This ensures that keys are updated and backward secrecy is maintained in network.

Forward Secrecy

Forward secrecy says that when a new node joins the network, it should not be able to decrypt the past encrypted traffic. On joining of new node, group leader generates new group key and sends to members of group encrypted with old group key and unicasts to new node encrypted with key shared between group leader and new node, ensuring forward secrecy.

Mutual Authentication

In proposed key management system, both new node and group leader authenticate each other mutually at the time of network joining. After successful mutual authentication, node can join the network. When two nodes wish to communicate, they also authenticate each other by sending their Digital Signature.

Man in Middle Attack

Man in the Middle (MITM) attack is a kind of active attack in which an attacker remains invisible between two nodes say A and B. Attacker splits the link into two links, one between node A and attacker and second, between attacker and second node B. Two nodes A and B think that they are communicating with each other, while they converse with attacker chairs in between them. Key management system proposed in [12] is susceptible to MITM attack; where an originator (new joining node) sends its public key to central node. In the response of request, central node generates a session key and sends to initiator, encrypted with initiator's public key. In this scheme, an attacker may exist in between initiator and central node; attacker can capture the public key of new node and send its public key to central node. Then central node shares the session key with attacker and attacker shares session key with initiator. But in planned key management system, both new node and group leader authenticate each other using challenge-response protocol. Hence, our key management system is not susceptible to MITM attack.

Proposed key management is a decentralized and hybrid scheme combining both symmetric and asymmetric cryptographic algorithms; which maintains forward and backward secrecy and provides security against many attacks such as reply attack, man in the middle attack etc. Limitation of proposed key management system is that it uses public key cryptography for key sharing and digital signature, which consumes more battery power in comparison of symmetric key cryptography.

REFERENCES

[1] L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network, vol. 13, no. 6, pp: 24–30, 1999.
[2] Meng Ge, Kwok-yan Lam, "Self-healing Key Management Service for Mobile Ad Hoc Networks", Proceeding of first International Conference on Ubiquitous and Future Networks", June, 2009.
[3] S. Yi and R. Kravets, "MOCA: Mobile Certificate Authority for Wireless Ad hoc networks," 2nd Annual PKI Research Workshop (PKI 03), 2003.
[4] H. Y. Luo, J. J. Kong, P. Zerfos, S. W. Lu, and L. X. Zhang, "Ursa: Ubiquitous and robust access control for mobile ad hoc networks, " IEEE/ACM Transactions on Networking, vol. 12, no. 6, pp:1049–1063, 2004.
[5] Mhd. Al-Shurman, Seong-Moo, Yoo, Bonam Kim, "Distributive Key Management for Mobile Ad Hoc Networks", International Conference on Multimedia and Ubiquitous Engineering, pp: 533-536, 2008.
[6] R. Blom, "Optimal class of symmetric key generation systems", Proceeding of the EUROCRYPT 84 workshop on Advances in Cryptology: Theory and Application of Cryptographic Techniques, pp: 335-338, December 1985, Paris, France.
[7] N. Kettaf, H. Abouaissa, P. Lorenz, "An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks", Springer, Telecommunication System, vol-37, pp: 29-36 , February 2008.
[8] H. Nam Nguyen, H. Morino, "A Key Management Scheme for Mobile Ad hoc Networks Based on Threshold Cryptography for Providing Fast Authentication and Low Signaling Load", EUC Workshops-2005, LNCS 3823, pp: 905-915, 2005.
[9] Zhu Lina, Zhang Yi, Feng Li, "Distributed Key Management in Ad hoc Network based on Mobile Agent", Proceeding of 2nd IEEE International Symposium on Intelligent Information Technology Application, vol. 1, pp: 600-604, 2008.
[10] G. A. Safdar, C. McGrath, M. McLoone, "Limitations of Existing Wireless Networks Authentication and Key Management Techniques for MANETs", Proceeding of 7th IEEE International Symposium on Computer Networks, pp: 101-107, 2006.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

[11] Yang Ya-Tao, Zeng Ping, and Fang Yong, Chi Ya-Ping., "A Feasible Key Management Scheme in Ad hoc Network", Proceeding of 8th IEEE International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp: 300–303, 2007.
[12] Azzendine Boukerche and Yonglin Ren, "The Design of a Secure Key Management System for Mobile Ad Hoc Networks", The 33rd IEEE Conference on Local Computer Networks, pp: 302-327, October, 2008.
[13] D. Cerri and A. Ghioni, "Securing AODV: The A-SAODV Securing Routing Prototype", IEEE Communication Magazine: Security in Mobile Ad hoc and Sensor Networks, vol-46, pp: 120-125, February, 2008.
[14] W. Huang, Y. Xiong, and D. Chen, "DAAODV: A Secure Ad hoc Routing Protocol based on Direct Anonymous Attestation", Proceeding of International Conference on Computational Science and Engineering, August, vol-2, pp: 809-816, 2009.
[15] Xukai Zou, Byrav Ramamurthy, "A Simple Group Diffie-Hellman Key Agreement Protocol without Member Serialization", Computational and Information Science, LNCS-3314, pp: 725-731, 2004.
[16] P. Papadimitratos, and Z. Haas, "Secure Routing for Mobile Ad hoc Networks", Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation, January, 2002.
[17] Y.C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks", Proceeding of 8th Annual International Conference on Mobile Computing and Networking, (MobiCom 02), September 2002, pp: 12-23,.
[18] J. Liu, F. Fu, J. Xiao and Y. Lu, "Secure Routing for Mobile Ad Hoc Networks", Proceeding of 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, vol-3, 2007, pp: 314-318.
[19] L. Buttyan, and I. Vajda, "Towards Provable Security for Ad hoc Routing Protocols", Proceeding of 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, October 2005, pp: 94-105.
[20] G. Ács, L. Buttyán, and I. Vajda, "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, vol-5, November 2006, pp: 1533-1546.
[21] N. Kettaf, H. Abouaissa, P. Lorenz, "An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks", Springer, Telecommunication System, vol-37,February 2008, pp:29-36.
[22] Y.Chun Hu, A. Perrig and David B. Johnson, "Wormhole Attack in Wireless Networks", IEEE Journal on Selected Areas in Communication, vol. 24, February 2006, pp: 370-380.
[23] R.A. Raja Mahmood, A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV-Based Mobile Ad hoc Networks", International Symposium on High Capacity Optical Networks and Enabling Technologies, November 2007, pp: 1-6.
[24] A. K. Shukla, N. Tyagi, "A New Route Maintenance in Dynamic Source Routing Protocol", IEEE International Symposium on Wireless Pervasive Computing, January, 2006.
[25] Kamal Kumar Chauhan and Amit Kumar singh sanger,"Securing Mobile Ad hoc Networks: Key Management and Routing", International Journal on Adhoc Networking System(IJANS) Vol.2 No.2,April 2012.

BIOGRAPHY

C. Mohammed Gulzar received his M.Tech degree in CSE from VTU, Belgaum, in 2008. Currently he is working as an Associate Professor in Dr. K.V. Subba Reddy institute of Technology, Kurnool, AP, India. He has 11 years of experience in teaching. His area of interest includes adhoc and wireless sensor networks.

Dr.P.Nageshwar received his Ph.D from MJPRU, Bareily, Uttar Pradesh. Currently he is working as an Assistant Professor in the department of Computer Applications at M.V.S Govt. Degree College, Mahabubnagar. He has more than 13 years of teaching experience. His area of interest includes Cloud Computing, Ad hoc Networks and Data Mining.

S. Imran Pasha received M.Tech from Samskruti College of Engineering & Technology, JNTUH, Hyderabad. Currently he is working as an Asst. Professor in the Department of CSE at Dr. KV. Subba Reddy Institute of Technology, Kurnool, A.P. He has more than 5 years of teaching experience. His area of interest includes Image Processing, Adhoc Networks and Data Mining.