International Journal of Soft Computing 9 (3): 183-188, 2014
ISSN: 1816-9503

An Optimized Color-Based Key Generation Algorithm for Secure Group Communications in MANETs

[1]B. Gopalakrishnan and [2]A. Shanmugam
[1]Department of Computer Applications, [2]Bannari Amman Institute of Technology,
638401 Sathyamangalam, Tamil Nadu, India

Abstract: An efficient and optimized secure group communication plays a vital role in many emergency communication. The operations on group key management protocol like joining or leaving the group dynamically and rekeying the group key when changes happen in the group are performed in many protocols. In the proposed system, a trust node is elected and a contributory group key is generated using the 24 bit color values (RGB) that provides a secure communication of messages among the group members in the dynamic environment through Diffie Hellman key exchange. The proposed system also reduces the cost of rekeying the group key when the mobility of the node increases. It was simulated to analyze the various issues related to group key management protocols like reliability, cost of contracting the group key when member join or leave the group dynamically, membership duration on re-keying overhead, inter-move variation on decryption/re-encryption overhead with member arrival duration. The above parameters are analyzed with respect to various other group key generation protocols and results are produced. The proposed system provides an optimized secure group key generation protocol for MANETs.

Key words: Group key, color value RGB, contributory key management, join or leave, rekeying MANETs

INTRODUCTION

Group communication is a security paradigm for many emerging network applications requiring a collaborated output from various peers. Many protocols have been proposed, designed and implemented to ensure the security issues in group communications like group authentication, group authorization and access control, group accountability and non-repudiation, group privacy and anonymity, group message integrity and confidentiality and group survivability and availability. In this group, key management protocols (Gharout *et al*., 2012) are been used to have secure communication among the group, members to ensure that the messages that are transferred among the group members in an authenticated way and privacy is maintained among the group members.

In many group-oriented scenarios such as video conferences and collaborative applications, secure group communication is of great importance since most communication occurs over insecure networks. A group key agreement protocol (Rafaeli and Hutchison, 2003; Harney and Muckenhirn, 1997; Wong *et al*., 2000; Hegland *et al*., 2006) enables a group of users to establish a shared secret key to achieve message confidentiality and integrity thus it plays an important role in achieving secure group communications. The group communication protocol (Jain and Umang, 2012; Gharout *et al*., 2012) has different approaches to Group Key Management (GKM) that are divided into three main classes:

Centralized group key management protocols: A single entity is employed for controlling the whole group, hence, a group key management protocol seeks to minimize storage requirements, computational power on both client and server sides and bandwidth utilization.

Decentralized architectures: The management of a large group is divided among subgroup managers, trying to minimize the problem of concentrating the work in a single place.

Distributed key management protocol: There is no explicit KDC and the members themselves do the key generation (Jain and Umang, 2012). All members can perform access control and the generation of the key can be either contributory, meaning that all members contribute some information to generate the group key or done by one of the members.

In this study, researchers have considered distributed key management protocol with contribution from the group members in generating the group key. A trust node (Al Shayeji *et al*., 2011; Cho *et al*., 2010)

Corresponding Author: Gopalakrishnan, Department of Computer Applications, 638401 Sathyamangalam, Tamil Nadu, India

is elected among the group members in considering battery power and mobility of the node. Each member in the group is assigned a private key using a color value RGB (Red Green Blue) and a group key is established among the group members by communicating the private key among the group. The join and leave request is sent to trusted node to assign the private key and rekeying will take place among the group members to generate the new group key.

Literature review: Many researchers have proposed many protocols related to group communication, Banerjee and Bhattacharjee (2000) proposed a management scheme based on a clustering protocol and a hierarchy of keys. All members are divided into several clusters in a layer. In each cluster, a cluster header will be selected and be a cluster member of the upper layer. This process is repeated until there is only one cluster member in the layer. The clustering protocol is deployed to cluster the members in each layer such that when a membership changes, only one cluster in each layer requires its associated keys to be updated. It was demonstrated that for an individual membership change, the overheads incurred by group members are constant with respect to the group size. In addition, for a bulk membership change, the processing and communication overheads at the key server are logarithmic with respect to the group size.

The schemes developed by Steiner *et al.* (2000) and Kim *et al.* (2000) belong to the Diffie-Hellman algorithm extended contributory key management. Instead of utilizing a trusted server to generate and distribute group keys, these schemes extend the well-known Diffie-Hellman Key Exchange algorithm to support group key agreement and thus lead to a rekeying cost proportional to the group size.

Amir *et al.* (2004) secured group communications with a secure service from the proposed robust and contributory key agreement protocol and the virtual synchrony semantics. The proposed protocol enhances the group Diffie-Hellman key agreement in two ways: first, it can mitigate the member serialization problem that requires the group key to be constructed or rekeyed in a serial ordering; second, it incorporates a membership protocol such that it is aware of any membership changes during the key generation and rekeying processes.

Sun and Liu (2007) proposed Multi-Group (MG) key management scheme to construct the logical key graph by integrating key trees of all members. Each authorized member holds a set of keys associated with the nodes from the leaf node to the root node in the key graph. The access privilege for each member is determined by the possessed set of keys. The scheme can provide forward and backward secrecies when a member changes its access privileges (or leaves the group) because the set of keys and resources associated with that member are reassigned (or withdrawn). It was shown that overheads caused by the rekeying incidents are greatly reduced. In addition, the scalability and complexity of the scheme is improved.

The most suitable solution to provide the services among which authentication, data integrity and data confidentiality is the establishment of a key management protocol (Bouassida *et al.*, 2008). Traffic Encryption Key (TEK) is used for generation and distribution of all the members in a group. Therefore, legal members can only receive the multicast flow which is sent by the group source and other members are not allowed to receive the flow.

A new group key management protocol for wireless communication ad hoc networks was stated by Rahman and Rahman (2008). They put forth a well-organized group key distribution (most commonly known as group key agreement) protocol which is based on multi-party Diffie-Hellman group key exchange and which is also password authenticated. The basic idea of the protocol is to securely construct and distribute a secret session key, K, among a group of nodes/users who want to communicate among themselves in a secure manner.

Rong *et al.* (2008) proposed pyramidal security model to safeguard the multi security-level information sharing in one co-operation domain. As a prominent feature, a pyramidal security model contains a set of hierarchical security groups and multicast groups. To find an efficient key management solution that covers all the involved multicast groups, they developed the following three schemes for the proposed security model: separated star key graph, separated tree key graph and integrated tree key graph. Performance comparison demonstrates that the scheme of integrated tree key graph has advantages over its counter parts.

Lima *et al.* (2009) introduce the most relevant survivable MANET initiatives where either preventive or reactive defences are combined with tolerant ones. For each one, they are correlated in terms of requirements and properties.

Teng and Wu (2012) provides a security model for a certificate less group key agreement protocol and proposes a constant-round group key agreement protocol based on CL-PKC. It does not involve any signature scheme which increases the efficiency of the protocol. It formally proven that the protocol provides strong AKE-security and tolerates up to n-2 malicious insiders for weak MA-security. The protocol also resists key control attack under a weak corruption model.

Researchers modified Burmester-Desmedt (BD) protocol for group key agreement in his protocol and enhance it to dynamic setting where a set of users can leave or join the group at any time during protocol execution with updated keys . In contrast to BD protocol he suggested DB (Dutta and Barua, 2008) protocol that is more flexible than BD protocol in dynamic environment and also reduces the number of rounds one less than BD protocol.

Lin and Lee (2010) proposes a key management scheme using Shamir's secret sharing scheme to construct an Autonomous Key Management (AKM) hierarchy structure. However, researchers modifies the secret sharing scheme and apply it to AKM for reducing communication and computation cost. An efficient attribute based signature (Zhang *et al*., 2012) based on cipher text-policy in attribute based encryption is proposed in group key management protocol the peers matches the attribute can contribute in group key generation.

Kamal (2013) proposed a polynomial-based key management scheme for secure intra-group and inter-group communication. He also proposed new approach in group forward and backward secrecy that is a node leaves a group, it can easily compute the new intra-group key based on its old key and the publicly broad-casted data. Similarly, researchers also show that when a node joins a group, it can discover the old keys.

This research is an extension of Teo and Tan's Circular Hierarchical Model for fixed number of group members. This protocol (Kumar *et al*., 2012) secures against replay, masquerading, spoofing, chosen ciphertext and impersonation attacks because of proper authentication and digital signatures. It is more suitable and well suited for low computational mobile devices with minimum delay.

A new GKM scheme for multiple multicast groups, called the Master Key Encryption Based Multiple Group Key Management (MKE-MGKM) (Park *et al*., 2013) scheme. It is shown that the MKE-MGKM scheme can reduce the storage overhead of a Key Distribution Center (KDC) by 75% and the storage overhead of a user by upto 85 and 60% of the communication overhead atmost, compared to the existing schemes. Seba *et al*. (2012) proposed a fully distributed and self-stabilizing Clustering algorithm for key management in MANETs where each cluster is an alliance.

MATERIALS AND METHODS

Proposed system: In the proposed system, the group key is generated in a contributory key management scheme where each node in the group will participate in group key generation. The protocol uses a 24 bit color value based on Red Green Blue (RGB) each node has a common red and green color value and BLUE value will be unique for each node in the group (Table 1 and Fig. 1).

Table 1: Node structure

Attribute	Description	Memory
Nid	Node identity	8 bit
Rvalue	Common value to group members	8 bit
Gvalue	Common value to group members	8 bit
Bvalue	Private key unique	8 bit
Gkey	Group key	8 bit
Tid	Trust identity	8 bit
Pvalue	Calculated in the node as public key value	8 bit
TBvalue	Trust node blue value used as prime number	8 bit
Count	No. of reachable nodes	8 bit
Mvalue	Mobility value of the node	8 bit
Bper	Battery percentage	8 bit

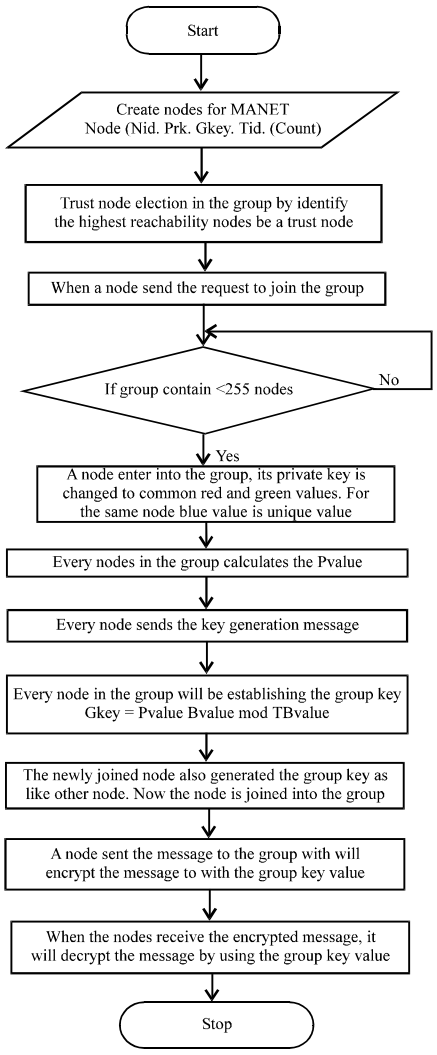

Fig. 1: The flow chart for proposed system

Initialization:

Step 1 (Create a node with the node structure): Create node (node structure)

Step 2 (Trust node election in the group):

- Each Node in the group will send a Trust Node Request (TNReq) message to one hop reachable nodes in the group

TNReq (Nid, Mvalue, Bper, Tid, Count)

- If (new. Mvalue<curr.Mvalue) AND (new.Bper >curr.Bper) then
  Assign curr.Tid = new. Nid.
- At every TNReq Message the count value at each node will be incremented by one for unique node id that is received by that node
- The node having Nid equal to Tid and count = max will be treated as a trusted node for that group

Step: 3 (Assigning keys to group members):

- In assigning the key researchers consider RED-8-bit value (Rvalue), GREEN-8-bit value Gvalue, BLUE-8-bit value Bvalue (RGB) 24 bit color values
- Trust node will be assigned a Bvalue as Prime no, Gvalue less than Bvalue, Rvalue greater Bvalue
- Trust node sends TNRes to every node in the group that participated in the trust node election

TNRes (Nid, Rvalue, Gvalue, Bvalue, TBvalue)

Where Nid¬Trust node id, Rvalue¬same Rvalue as in Trust node, Gvalue¬same Gvalue as in Trust Node, Bvalue¬incremented by 1 on B-value of the trust node for every node in the group and TBvalue¬Bvalue in trust node

- Every node will be having Rvalue, Bvalue common to all nodes in the group where Bvalue will be unique to everyone in the group

Step 4 (Generating the group key):

- Every node in the group calculates the Pvalue with Gvalue, TBvalue and Bvalue as:

$$Pvalue = Gvalue^{TBvalue} \text{ Mod } Bvalue$$

- Every node sends the Key Generation message KGen (Nid, Pvalue, Tid) to every node in the group. This message is used to esatbilsh the group key in individual nodes
- Every node in the group will establish the group key (Gkey) using Pvalue Bvalue and TBvalue as:

$$Gkey = Pvalue^{Bvalue} \text{ Mod } TBvalue$$

- The Encryption and Decryption are performed using the group key to have secure communication among the group members

Step 5 (Node joining a group):

- A node is created with the node structure and sends the JReq message to all the nodes that are reachable from that node

Create node (node structure);
JReq (Nid, M-value, Bper, Tid, Count);

- When the trust node receives the JReq message. it checks whether count reaches 255 (i.e., max number of nodes in the a group). It sends TNRes as node cannot be joined
  Else

TNRes (Nid, Rvalue, Gvalue, Bvalue, Tbvalue)

Where Nid¬trust node id, Rvalue¬same Rvalue as in trust node, Gvalue_ same Gvalue as in trust node, Bvalue_incremented by 1 on Bvalue of the trust node for every node in the group and TBvalue_Bvalue in trust node

- Rekeying the joining/leaving process is performed for the newly joined node

Step 6 (Node leaving the group):

- The node wants to leave the group will send a LReq (node structure) to the trust node with its node structure
- The trust node reinitialize node structure values that already present in the node. The Node id and all other attributes reset to the initial value
- The rekeying is done with the remaining nodes in the group

Step 7 (Rekeying of the join/leave process):

- Newly joined node in the group calculates the Pvalue with Gvalue, TBvalue and Bvalue as:

$$Pvalue = Gvalue^{TB\text{-}value} \text{ Mod } Bvalue$$

- Newly joined node in the group will be establishing the Group key (Gkey) using Pvalue Bvalue and TBvalue as:

$$Gkey = Pvalue^{B\text{-}value} \text{ Mod } TBvalue$$

- The Encryption and Decryption are performed using the group key to have secure communication among the group members

RESULTS AND DISCUSSION

The simulation is performed with nodes created dynamically in a group with a specific node structure. The attributes are set as mobility as random way point, the routing protocol as DSR, Wireless connection as 802.11b WLAN, Data transfer as CBR (Constant Bit Rate) and performances are analyzed with respect to join/leave the group vs. rekeying time, No. of nodes vs. group key establishment time, mobility vs. group key establishment time, trust node establishment time vs. mobility.

Trust node establishment time vs. mobility: The trust node to be elected when the group is formed or there is failure in the trust node or it wants to move out of the group then a new trust node to be elected in the group. The analysis corresponds to time taken to establish a new trust node when any one condition happens as said above in the MANET, the analysis is performed with different protocols on mobility and the time taken to elect a new trust node in the group. The proposed system has constant increase in time with respect to the increase in mobility percentage (Fig. 2).

Number of nodes vs. group key establishment time: The simulation is performed by increasing the number of nodes in the group to identify the time taken to establish

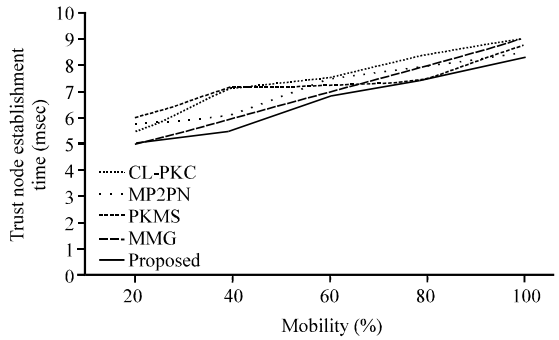

Fig. 2: Trust node establishment time vs. mobility

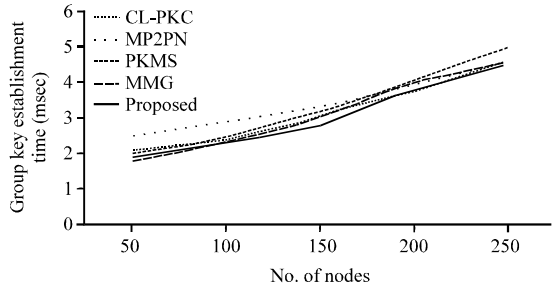

Fig. 3: No of Nodes vs. group key establishment time

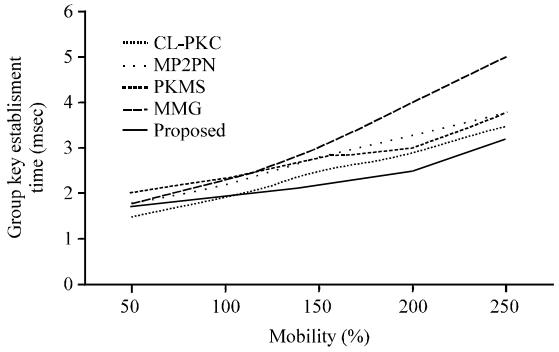

Fig. 4: Mobility vs. group key establishment time

the group key. It was found that the proposed system has O(n) time to establish the group key where n refers to number of nodes (Fig. 3).

Mobility vs. group key establishment time: The mobility play a major role in MANETs the proposed system is compared with other protocol to ensure the mobility effect less in the proposed system with respect to group key establishment time (Fig 4).

Joining or leaving vs. rekeying time: The simulation shows that the increase in number of nodes joining or leaving the group at particular time doesn't have much impact on the rekeying process in the group (Fig. 5).

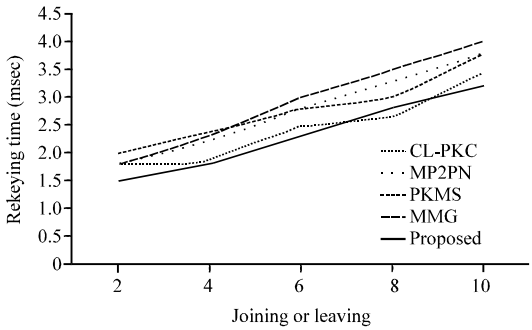

Fig. 5: Trust node vs. rekeying time

CONCLUSION

The secure group communication in MANETS can be achieved by many group key management protocol. The proposed system ensures the fast and efficient group key management scheme to send and receive messages among the group members in a secured way and also optimizes the rekeying process during the member joining or leaving the group dynamically. It also proves that proposed system is efficient and optimal when compared with other group key management protocols. The system is more efficient for intra group communication in MANETs and certain modifications to be made in the proposed system perform secure inter group communication in MANETs.

REFERENCES

Al Shayeji, M.H., A.R.R. Al-Azmi, A.A.R. Al-Azmi and M.D. Samrajesh, 2011. Analysis and enhancements of leader elections algorithms in mobile ad hoc networks. ACEEE Int. J. Network Secur., 2: 19-24.

Amir, Y., Y. Kim, C. Nita-Rotaru, J.L. Schultz, J. Stanton and G. Tsudik, 2004. Secure group communication using robust contributory key agreement. IEEE Trans. Parallel Distrib. Syst., 15: 468-480.

Banerjee, S. and B. Bhattacharjee, 2000. Scalable secure group communication over IP multicast. IEEE J. Sel. Areas Commun., 20: 1511-1527.

Bouassida, M.S., I. Chrisment and O. Festor, 2008. Group key management in MANETs. Int. J. Network Secur., 6: 67-79.

Cho, J.H., A. Swami and I.R. Chen, 2010. A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 13: 562-583.

Dutta, R. and R. Barua, 2008. Provably secure constant round contributory group key agreement in dynamic setting. IEEE Trans. Inform. Theory, 54: 2007-2025.

Gharout, S., A. Bouabdallah, Y. Challal and M. Achemlal, 2012. Adaptive group key management protocol for wireless communications. J. Universal Comput. Sci., 18: 874-898.

Harney, H. and C. Muckenhirn, 1997. Group Key Management Protocol (GKMP) architecture. Network Working Group Request for Comments: 2094, Category: Experimental, SPARTA Inc., July 1997. http://tools.ietf.org/pdf/rfc2094.pdf.

Hegland, A.M., E. Winjum, S.F. Mjolsnes, C. Rong, O. Kure and P. Spilling, 2006. A survey of key management in ad hoc networks. IEEE Commun. Surv. Tutorials, 8: 48-66.

Jain, D. and Umang, 2012. Performance comparison of distributed group key management protocol based on region based group key management. Proceedings of the National Conference on Communication Technologies and its Impact on Next Generation Computing, November 9-11, 2012, Foundation of Computer Science, New York, USA., pp: 4-8.

Kamal, A.A., 2013. Cryptanalysis of a polynomial-based key management scheme for secure group communication. Int. J. Network Secur., 15: 59-61.

Kim, Y., A. Perrig and G. Tsudik, 2000. Simple and fault-tolerant key agreement for dynamic collaborative groups. Proceedings of the 7th ACM Conference on Computer Communication Security, November 1-4, 2000, Athens, Greece, pp: 235-244.

Kumar, A., A. Aggarwal and Charu, 2012. Efficient hierarchical threshold symmetric group key management protocol for mobile ad hoc networks. Proceedings of the 5th International Conference on Contemporary Computing, August 6-8, 2012, Noida, India, pp: 335-346.

Lima, M.N., A.L. dos Santos and G. Pujolle, 2009. A survey of survivability in mobile ad hoc networks. IEEE Commun. Surv. Tutorials, 11: 66-77.

Lin, C.H. and C.Y. Lee, 2010. Modified autonomous key management scheme with reduced communication/computation costs in MANET. Proceedings of the International Conference on Complex, Intelligent and Software Intensive Systems, February 15-18, 2010, Krakow, Poland, pp: 818-821.

Park, M.H., Y.H. Park, H.Y. Jeong and S.W. Seo, 2013. Key management for multiple multicast groups in wireless networks. IEEE Trans. Mobile Comput., 12: 1712-1723.

Rafaeli, S. and D. Hutchison, 2003. A survey of key management for secure group communication. ACM Comput. Surv., 35: 309-329.

Rahman, R.H. and L. Rahman, 2008. A new group key management protocol for wireless ad-hoc networks. Int. J. Comput. Inform. Sci. Eng., 2: 74-79.

Rong, B., H.H. Chen, Y. Qian, K. Lu, R.Q. Hu and S. Guizani, 2009. A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study. IEEE Trans. Veh. Technol., 58: 398-408.

Seba, H., S. Lagraa and H. Kheddouci, 2012. Alliance-based clustering scheme for group key management in mobile ad hoc networks. J. Supercomput., 61: 481-501.

Steiner, M., G. Tsudik and M. Waidner, 2000. Key agreement in dynamic peer groups. IEEE Trans. Parallel Distrib. Syst., 11: 769-780.

Sun, Y. and K.J.R. Liu, 2007. Hierarchical group access control for secure multicast communications. IEEE/ACM Trans. Networking, 15: 1514-1526.

Teng, J. and C. Wu, 2012. A provable authenticated certificateless group key agreement with constant rounds. J. Commun. Networks, 14: 104-110.

Wong, C.K., M. Gouda and S.S. Lam, 2000. Secure group communications using key graphs. IEEE/ACM Trans. Networking, 8: 16-30.

Zhang, G., X. Fu and C. Ma, 2012. Attribute-based authenticated group key management protocol for mobile peer-to-peer network. China Commun., 9: 68-77.