EETSS: Energy Efficient Transitive Signature Scheme for Secure Group Communication in MANETs

B. Gopalakrishnan [#1], Dr. A. Shanmugam [*2],

[#] Department of Computer Applications , Bannari Amman Institute of the Technology
Sathyamangalam Erode Dt Tamilnadu India
[1] bgopal1977@gmail.com.
[*] Principal
Bannari Amman Institute of the Technology
Sathyamangalam Erode Dt Tamilnadu India
[2] dras_bit@yahoo.com

***Abstract*— A secure group communication in Mobile Ad-Hock Networks is challenging due to the mobility and limitations in computational and battery power of the nodes. This can be achieved by multicast routing protocol that ensures security through key management schemes. In this paper we proposed an energy efficient multicast routing protocol to establish the group in MANETS. In order to preserve security in data transmission, transitive signature scheme was introduced to enhance the security among the group nodes. The nodes may join/leave the group dynamically. To achieve this, the rekeying operation is performed for every change that happens in the group. The performance analysis on computational and communicational cost is done by varying group size and energy level of the nodes. This scheme results in low computational cost with respect to other protocols.**

Keyword- Energy efficient Multicast Routing Protocol, Secure Group Communications, Transitive Signature scheme, MANET.

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies. In mobile ad hoc network, nodes can directly communicate with all the other nodes within their radio frequency range; whereas nodes that are not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as mobile ad hoc network. These properties make MANET very suitable for group communications. This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website.

A. Multicast Routing Protocols

Generally there are two types of multicast routing protocols in wireless networks. Tree-based multicast routing protocol, Mesh-based multicast protocol [2-5]. Mesh-based multicast routing protocols are more suitable for Group Communication in MANETs. In Dynamic Core Multicast Routing Protocol the nodes are classified as Active node, Passive Node, Core Active Node.

Security requirements for secure group communication in MANETs are as in the Fig 1 follows:

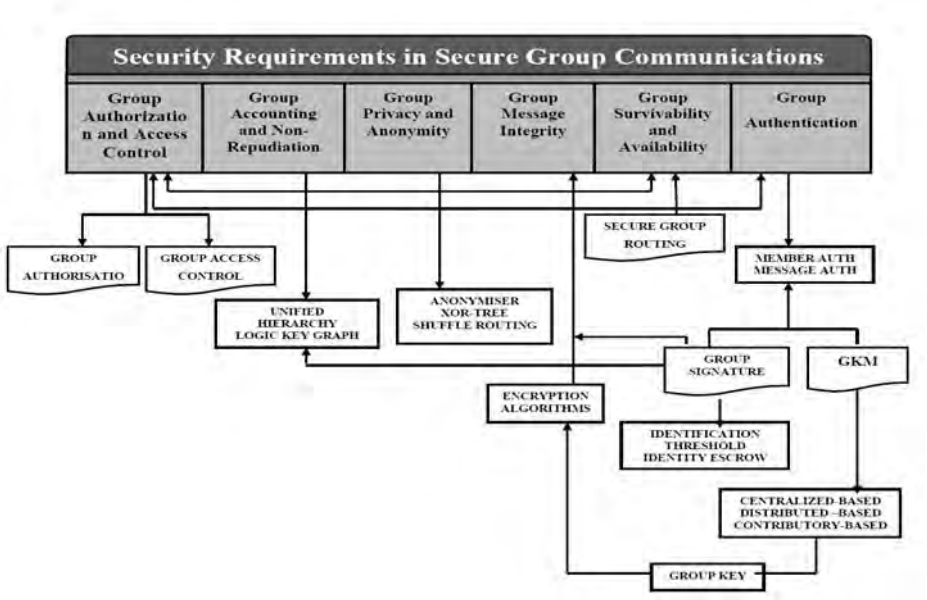

Fig 1. Security Requirements for Secure Group Commmunication

B. A transitive signature scheme

A transitive signature scheme [1] TS = (TKG, TSign, TVf, Comp) is specified by four polynomial time algorithms and the functionality is as follows:

The randomized key generation algorithm TKG takes input 1^k,where $k \in$ N is the security parameter, and returns a pair (*tpk, tsk*) consisting of a public key and matching secret key.

The signing algorithm TSign, which could be stateful or randomized (or both), takes input the secret key *tsk* and *nodes i, j* $\in$ N, and returns a value called an original signature of edge {i, j} relative to *tsk*. If statefull, it maintains state which it updates upon each invocation.

The deterministic verification algorithm TVf, given *tpk*, no des *i, j* $\in$ N, and a candidate signature σ, returns either 1 or 0. In the former case we say that σ is a *valid* signature of edge *{i, j}* relative to *tpk*.• The deterministic *composition* algorithm Comp takes *tpk*, no des *i, j, k* $\in$ N and values σ1, σ2 to return either a value σ or a symbol $\perp$ to indicate failure.

This paper is organized as follows Section 2 discuss about many Secure Group Communication Protocols that are developed in the recent years to provide secure data communication with in the group members[18]. The Section 3 proposes Energy Efficient Secure Group Communication through Dynamic core Multicast routing protocol to from the group. Transitive signature scheme is involved in the routing process to ensure secure data/ information exchange between the group members. Due to mobility of the nodes, it may join or leave the group at any time, to maintain security the rekeying operation is done on the nodes. Section 4 Simulation is performed with our proposed system to establish a secure group communication in MANETs with certain assumptions in the wireless ad hoc networks. It also analyses various protocols mentioned in related works with our proposed protocol to confirm our protocol benefits than the other protocols.

II. RELATED WORKS

The schemes developed by M. Steiner, G. Tsudik, and M. Waidner [6]–[7] 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. [8] 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 itis aware of any membership changes during the key generation and rekeying processes. Rony et al [9] they 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: 1) separated star key graph; 2) separated tree key graph, and 3) integrated tree key graph. Performance comparison demonstrates that the scheme of integrated tree key graph has advantages over its counter parts.

JikaiTeng and Chuankun[10] 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. The author 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 [11] protocol that is more flexible than BD protocol in dynamic environment and also reduces the number of rounds one less than BD protocol.

Huihua Zhou et. al [12] proposed scheme, an ad hoc network is divided into a control group and cell groups. In addition, the proposed hybrid key establishment scheme employs the implicitly certified public keys method to achieve authenticated key agreement between group member and group controller. This method can avoid the need to manage public key certificates. An efficient attribute based signature [13] based on ciphertext-policy in attribute based encryption is proposed in group key management protocol, the peers matches the attribute can contribute in group key generation. A new GKM scheme for multiple multicast groups, called the master-key-encryption-based multiple group key management (MKE-MGKM) [14] scheme. It is shown that the MKE-MGKM scheme can reduce the storage overhead of a key distribution centre (KDC) by 75 percent and the storage overhead of a user by upto 85 percent, and 60 percent of the communication overhead at most, compared to the existing schemes.

Abdel Alim Kamal [15] proposed Polynomial-Based Key Management Scheme (PKMS) 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, we also show that when a node joins a group, it can discover the old keys. Yining Liu et. al [16] propose an improved authenticated key transfer protocol based on Shamir's secret sharing. The proposed protocol achieves key confidentiality due to security of Shamir's secret sharing, and provides key authentication by broadcasting a single authentication message to all members Furthermore, the proposed scheme resists against both insider and outsider attacks. Muhammad Imran Khan Khalil [17] proposed group key management approach, which further uses a symmetric group key for to communicate inside the cluster. Cluster head is responsible for the generation of group key and is responsible for the communication of other nodes throughout a secure path which uses public key cryptography scheme. Encryption of messages is used for group keys to communicate inside the cluster and within the group for secure communication. It also examines the system for proper authentication of public and private keys and evaluates the functioning of proposed methodology.

III. PROPOSED SYSTEM

A. Proposed System Model of EETSS

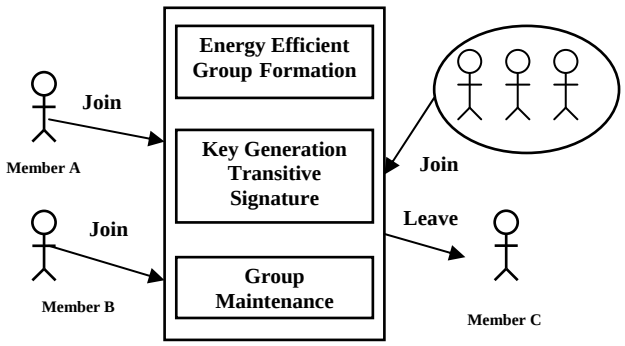

Fig 2 The Proposed Model of EETSS

1. Create a Node with Node Structure in the mesh topology.

TABLE I
NODE STRUCTURE

Notation	Description
N_i	i^{th} Node Identity
Gi	Group ID
Tpk	i^{th} Private key
Tsk	i^{th} Secrete key
Gkey	Group Key
EE	Two dimensional array(n:2)
NT	Node Type
TStamp	Timer Counter
BL	Battery Level in %

2. Initialization

Each node in the network is classified as Active Node or Passive Node by considering the battery level of the node. Assigning Node Type to every node in the mesh topology as Active Node or Passive Node by using the algorithm.

Pseudo code for assigning Node Type

```
// Let n be number of nodes in the network and BL be battery level
Percentage of the nodes in the network.
Node Type (n)
Begin
For i = 1 to n
Begin
Read the Battery Level of Ni
If (N[i]. BL < 50) then
N[i].NT = 'PN';
Else
N[i].NT = 'AN';
End
```

B. Group Formation using DCMP Protocol.

The Dynamic Core based Multicast Routing Protocol has two phases in the routing process as Route Discovery and Route Maintenance.

1. Route Discovery Phases:

In Route Discovery phases each Active Node (AN) in the network create a join request **JoinReq** message and floods to one hop neighbours in the Mesh network. The Receiving nodes will maintain a table having the node id, Energy Efficiency EE, Transitive Secrete Key (Tsk) of the sending node. The passive node just forwards the JoinReq message to its one hop neighbours. The Energy Efficiency EE is computed as follows

RECEIVE (EE) = SEND (JoinReq (Battery Level BL + Time taken to send message TStamp)).
JoinReq (Ni, BL, TStamp, Tsk);

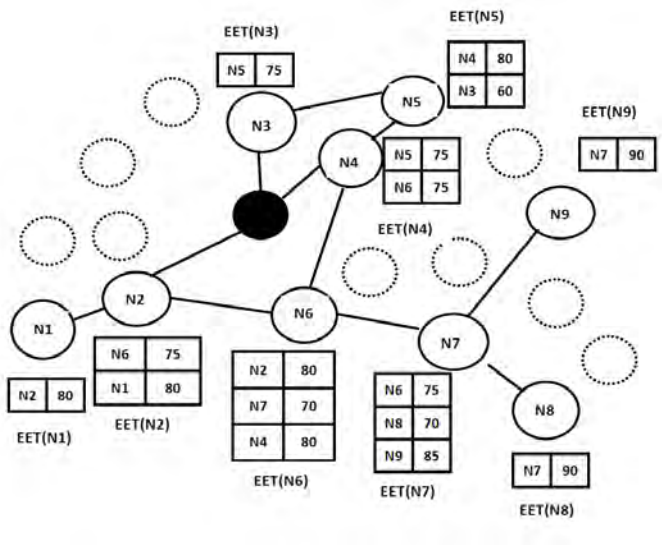

Fig 3 Group Formation through Energy Efficiency

The Active Node will not forward any JoinReq received from any other Active node in the network. When passive node wants to communicate in the group then it registers with Active node that has maximum EE in the one hop neighbour of the Passive node.

After completion of join request message the nodes will start creating ReplyAck message and find the max (EE) node in their table and send the ReplyACK to that node and deletes all the other entries in the table. After this process there exists only one path between each node in the Network. These nodes form a group with energy efficient group nodes to compute group key to have secure communication among the group nodes.

2. Group Key Generation Algorithm

The transitive signature scheme was employed to generate group key in the Energy Efficient Secure Group communication in MANETs. To accomplish this task the node having least node id will create a GReq message and compute TKG (N_i) and send it through the node specified in the Energy Efficiency Table (EET).

Procedure for Group key Generation:

Creating the private (Tpk) and secrete (Tsk) key through transitive signature based key generation algorithm (TKG).

(Tpk, Tsk) ← TKG (N_i);

Each node on receiving the GReq will store the Sender node id and the corresponding Tsk value to compute Group key

If Node Nj receives GReq message from Ni. Then Group key is computed as

GKey N_j = (N_i .Tsk mod N_j.Tpk)

The receiving node creates a GReplyAck (Nid, GKey) message and sends it to the requested node.

Pseudo code for Transitive Signature Group Key (TKG)

TGK (N_i)
Begin
Take any two large prime p and q such that q divides p-1;
Two generates g = $h^{(p-1)/q}$ mod p Where h is any integer with 1< h< p-1
x = pseudo randomly generated integer with 0 < x< q;
y = g^x mod p;
k = pseudo randomly generated integer with 0 < k< q;
Tpk = (g^x mod p) mod q;
*Tsk = (k^{-1} + x * r) mod q;*
Return (Tpk,Tsk);
End

3. Route Maintenance Phase:

A Node joining the group

The group is already created and if a new Active Node wants join the group then it sends a JoinReq (Ni, BL, TStamp, Tsk,) to one hop neighbours in the network and update the EET of the receiving nodes. The receiving node sends a ReplyAck message by choosing the highest value in the Energy Efficiency Table (EET). The group key generation algorithm is performed with the new group.

The New node is Passive Node that wants to send any information to the existing group then the passive node send registration request (RReq) to one hop neighbours in the network that will be treated as Core Active Node and it act like a proxy to that passive node that requested and sends Ack message to that node.

Pseudo Code for a node joining a group G

JoinReq (Node N_i, Group G_j)

If (N_i. NT ==" AN) then
Begin
Send JoinReq to one hop neighbours in the group G_j.
For k = 1 to h // number of one hop neighbours of node N_i in the network
Begin
JoinReq (N_i, BL_i, $TStamp_i$, Tsk_i,)
Insert Node N_i details in the EET of each k node;
End
Invoke Group Key Generation algorithm
End

A node leaving the Group:

The node wants to leave the group will send an LReq message to the one hop neighbours in the network. The receiving nodes update the EET by removing the details of the node from the table entry entire row of the table values are deleted and removed from the table.

The Generation Key Generation Process is performed with the new updated table entries of the node.

Group key Generation (new node N_i);

Pseudo code for leaving a node from the group.

LeaveReq (Node N_i, Group G_j)

If (N_i. NT ==" AN) then
Begin
Send LReq to one hop neighbours in the group G_j.
For k = 1 to h // number of one hop neighbours of node N_i in the network
Begin
LReq (N_i, BL_i, $TStamp_i$, Tsk_i,)
Delete Node N_i details in the EET of each k node;
End
Invoke Group Key Generation algorithm
End

IV. Simulation and Results

The above protocol Energy efficient Transitive Signature Scheme for Secure Group Communication (EETSS-SGC) is implemented in ns2 simulator. We evaluate the performance of the Transitive Signature scheme in DCMP routing protocol in simulation based experiment. We study their performance in more general setting and also compare the performance of our protocols with other approach such as CP-ABE [13] and PKMS[15] specified in the related works.

The following assumptions are made on NS2 Simulator:

```
ns_ node-config-adhocRoutingDCMP
                    -llType LL \
                      -macType Mac/802_11\
                      -ifqLen 50 \
                      -ifqType Queue/DropTail/PriQueue \
                      -antType Antenna/OmniAntenna \
                      -propType Propagation/Random Way Point \
                      -phyTypePhy/WirelessPhy \
                      -channelType Channel/WirelessChannel \
                      -topoInstance $topo
                      -agentTrace ON \
                      -routerTrace ON \
                      -macTrace OFF
```

A. A node Join operation with other protocols

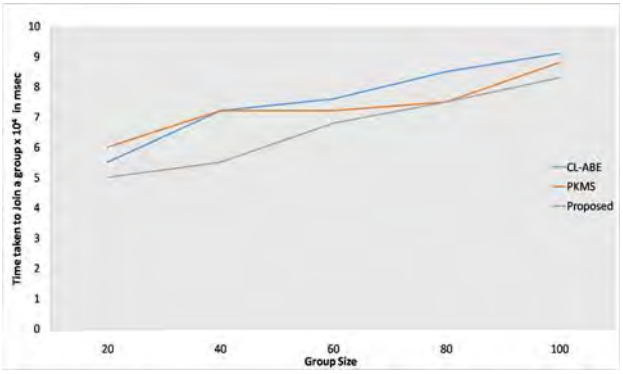

Fig. 4. Comparison of join operations with other protocols

The above Fig 4 shows the performance of protocol EETSS-SGC with other protocols. The y axis shows the time taken join operation and x axis shows the number of nodes (group size) participated in the group key generation. The time taken is normal i.e. O (n) when the size of the group size increases. The node join operation involves the energy efficiency path to construct the group key.

B. A node Leave operation with other protocols

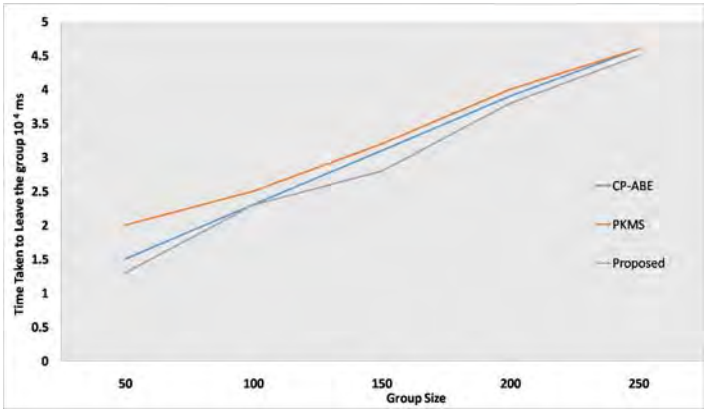

Fig. 5. Comparison of leave operation with other protocols

The above Fig 5 shows the time taken to reconstruct the group key when the node leaves the group is directly proportional to the size of the group members. The leaving operation takes less communication cost in the proposed system when the group size increase proportionately. The time complexity to construct the group key is O (n) where n is the no of nodes in the group.

C. Initial Group Formation Time

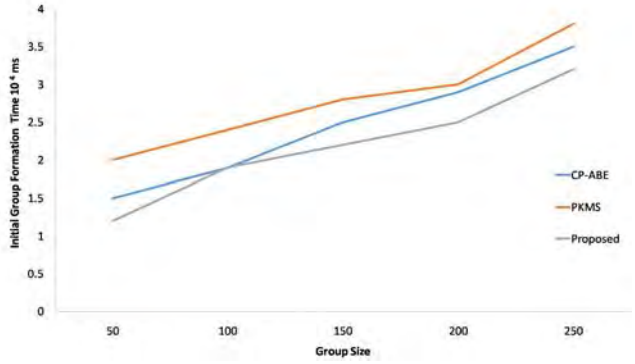

Fig. 6. Comparison initial group formation time with respect to group size

The above Fig 6 shows the time taken to form the group initially in the mesh network. It mainly involves the communicational cost to form the secure group using Energy efficient DCMP protocol to optimize the routing path of the group. Performance is similar for small group size whereas increase in group size will have more impact on other protocols.

D. Computational Performance

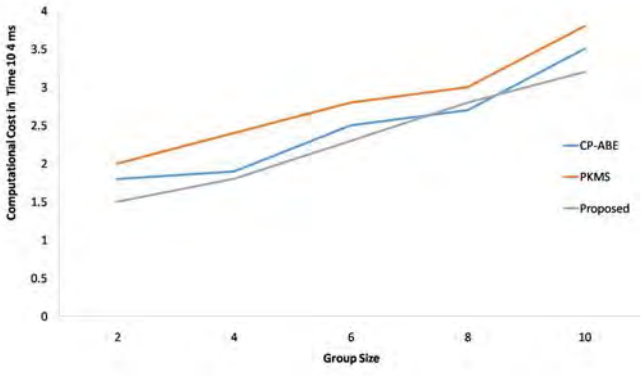

Fig. 6. Comparison Computational Cost Vs Group Size

The above Fig 6 shows the computational cost of the group key generation with respect to the Group Size. The computational cost comprises of the following.

Computational Cost = ∑ Generating (Tsk, Tpk) + Generating (Group key);

V. CONCLUSION

This paper proposed EETSS-SGC Energy Efficient Transitive Signature Scheme for Secure Group Communication that includes Dynamic Core based Multicast Routing Protocol (DCMP) for group formation. It also involves an energy efficient signature scheme called transitive signature scheme to ensure security in the data transmission. The collaborative group key is generated for secure group communication in MANETs and the rekeying is done due to the mobility of the nodes. The performance of the above protocol is compared with various signature based Group Key Management protocols in MANETs. This scheme proves to be more suitable for large group size and high mobility in the environment. It drastically reduces the communication cost incurred for secure group communication in MANETs.

REFERENCES

[1] Dang Nguyen Duc,_ Zeen Kim , Kwangjo Kim “A New Provably Secure Transitive Signature Scheme” Symposium on Cryptography and Information Security, The Institute of Electronics, Information and Communication Engineers ,Maiko Kobe, Japan, Jan.25-28, 2005.

[2] Jorjeta G. Jetcheva and David B. Johnson: "Adaptive Demand-Driven Multicast Routing in Multi-Hop Wireless Ad Hoc Networks", *InProc.of the 2nd ACM International Symposium on Mobile and Ad-hoc Networking & Computing (MobiHOC)*, 33 - 44, October (2001).

[3] Sung-Ju Lee, Mario Gerla, and Ching-Chuan Chiang: "On-Demand Multicast Routing Protocol", I*n Proc. of the Wireless Communications and Networking Conference (WCNC)*, 1298 - 1302, September (1999).

[4] Koushik Sinha, Bhabani P. SinhaM. Debasish Datta. An Energy-Efficient Communication Scheme for Wireless Networks: A Redundant Radix-Based Approach IEEE Transactions on Wireless Communications, VOL. 10, NO. 2, FEBRUARY 2011.

[5] Osamah S Badarneh and Michel Kadoch, (2009), “Multicast Routing Protocols in Mobile Ad Hoc Networks: A Comparative Survey and Taxonomy”, EURASIP Journal on Wireless Communications and Networking PP 1-42, 2009.

[6] M. Steiner, G. Tsudik, and M. Waidner, “Key agreement in dynamic peergroups,” IEEE Trans. Parallel Distrib. Syst., vol. 11, no. 8, pp. 769–780,Aug. 2000.

[7] Y. Kim, A. Perrig, and G. Tsudik, “Simple and fault-tolerant key agreementfor dynamic collaborative groups,” in Proc. ACM Conf. Comput.Commun. Security, Nov. 2000, pp. 235–244.
[8] AMIR Y., KIM Y., ROTARU C.N., SCHULTZ J.L., STANTON J., TSUDIK G.‘Secure group communication using robust contributory key agreement’, IEEE Trans. Parallel Distrib. Syst.,,15, (5), pp. 468–480, 2004.
[9] RONG et al.: Pyramidal security model for large-scale group-oriented computing in manets IEEE transactions on vehicular technology,pp 398-408 VOL. 58, NO. 1, JANUARY 2009
[10] JikaiTeng and ChuankunWuA Provable Authenticated Certificateless Group KeyAgreement with Constant RoundsJOURNAL OF COMMUNICATIONS AND NETWORKS, PP 104-110 VOL. 14, NO. 1, FEBRUARY 2012
[11] R. Dutta and R. Barua, “Provably secure constant round contributorygroup key agreement in dynamic setting,” IEEE Trans. Inf. Theory, vol.54, no. 5, pp. 2007–2025, May 2008.
[12] Huihua Zhou, Minghui Zheng, Tianjiang Wang” A Novel Group Key Establishment Scheme for MANETs” Published by Elsevier Ltd issue 15 PP 3388 –3395 2011,
[13] ZhangGuoyin , Fu Xiaojing Et al Attribute-Based Authenticated Group Key Management Protocol-to-Peer Network China Communication on Information Security .PP 68- 77, Vol 10 , 2012
[14] Min-Ho Park, Young-Hoon Park, Han-You Jeong and Seung-Woo Seo, “Key Management for Multiple Multicast Groups in Wireless Networks” IEEE Transactions On Mobile Computing, VOL. 12, NO. 9,PP 1712-1723, SEPTEMBER 2013.
[15] Abdel Alim Kamal,” Cryptanalysis of a Polynomial-based Key Management Scheme for Secure Group Communication”, International Journal of Network Security, Vol.15, No.1, PP.59-61, Jan. 2013.
[16] Yining Liu, Chi Cheng, Jianyu Cao and Tao Jiang. “An Improved Authenticated Group Key Transfer Protocol Based on Secret Sharing”, IEEE Transactions on Computers, 2013.
[17] Muhammad Imran Khan Khalil” Improve Quality of Service and Secure Communication in Mobile Adhoc Networks (Manets) Through Group Key Management”, International Review of Basic and Applied Sciences, Vol. 1 Issue.3, pp 107-115 August 2013.
[18] B. Gopalakrishnan1, T. V. P. Sundararajan 2 and Dr. A. Shanmugam “AGPM: An Authenticated Secure Group Communication Protocol for MANETs” ACEEE International Journal on Network Security, Vol 1, No. 1, pp 17-20 ,Jan 2010.