Multi Group Key Agreement Mechanism for Mobile P2P Wireless Networks

Mourad AMAD[1], Djamil AÏSSANI[2], Ahmed MEDDAHI[3] and Mustapha SAADI[4]
[1]Laboratory LAMOS, Bejaia University, Algeria, mourad_amad@gmail.com
[2]Laboratory LAMOS, Bejaia University, Algeria, lamos_bejaia@hotmail.com
[3]Institut Telecom/Telecom Lille 1, France, ahmed.meddahi@telecom-lille1.eu
[4]Bejaia University, Algeria, mustsaadi@yahoo.fr

***Abstract*—Secure and efficient communication among a set of mobile nodes is one of the most important aspect in P2P wireless networks. Security of various group-oriented applications requires a group secret shared between all participants. Several group key protocols have been presented in the literature to enable secrecy of communication among dynamic group of participants. However, most of them suffer from the scalability problem. In this paper, we propose a novel multi group key agreement mechanism for P2P wireless network. The proposed model is organized as several neighboring rings. Each group of peer belonging to the same ring has to agree on a contributed key, and the peer belonging to two adjacency rings have one key for each ring. Then, only a small set of nodes has to recalculate the key in case of join or leave operations.**
Key words: P2P wireless network, GKA, Secure communication.

I. Introduction

P2P Wireless networks have attracted significant attentions recently due to its wide applications in different areas (*eg. military applications, natural catastrophic detection ...*). P2P Wireless networks are composed of constrained devices communicating over wireless channels in the (*partial*) absence of any fixed infrastructure. Moreover, network composition is highly dynamic with devices leaving/joining the network quite frequently. It is characterized by an expensive communication (*devices with limited energy*), easy of interception of messages, and limited computational capabilities of devices. Secure communications in such networks is a challenge.

There are five main attributes of security [2]: availability, confidentiality, integrity, authentication and non reputation. Availability is to ensure that the network service survive despite denial of service attacks. Confidentiality ensures that information is passed only to authorized members of the network. Integrity is to guarantee that a message is transferred without getting corrupted. Authentication is to enable a node to identify the identity of the peer node it is communicating with. Non reputation is to ensure that a node can not deny having sent/received the message.

Group communication deals with packet delivery from one or more authorized senders to a large number of authorized receivers. Secure group communication (*providing confidentiality, authenticity and integrity of messages delivered between group members*) is an important Internet design issue since many applications like teleconference, real time information services, distributed interactive simulation and collaborative work are based upon a group communication model. Group communication confidentiality prevents non-group members from reading data exchanged within a secure communication session of the group. This confidentiality requires establishing and maintaining a common key between group members. This key, called group key or traffic encryption key (TEK) serves to encrypt/ decrypt message exchange within the group.

Almost all cryptography protocols are based on private keys or public keys. Public key based protocols have some inherent advantages over the private key protocols. However, it is well known that the private key based encryption protocols (*eg. DES, AES*) are much faster than the public key based protocols (*eg. RSA, ElGamal*). In this paper, we will concentrate on how to build a common private key for a group, so they can communicate securely, this problem is called GKA. The GKA is a mechanism that allows establishing a cryptographic key for a group of participants, based on each one's contribution. Then, the key can be used to secure canal communication. Many GKA protocols have been proposed in the literature, but most of them suffer from scalability, especially, for height dynamic networks.

In this paper, we propose a novel distributed multi group key agreement mechanism for peer to peer wireless networks where height dynamicity does not affect significantly the global system.
The rest of this paper is organized as follows: in section 2, we give related works on group key agreement. Section 3 introduces our proposed mechanism consisting of multi group key agreement for peer to peer wireless network. In section 4, we give performance evaluation of the proposed solution. Finally, we conclude and give some perspectives for future works.

II. Related Works

In general, the key establishment protocols can be classified into two types: key distribution protocols and key agreement protocols [3]. Key distribution protocols, sometimes called

as centralized key distribution protocols, they are generally based on a trusted third party (TTP). On the other hand, the key agreement protocols do not use a TTP, but on the group members for a general key agreement. The centralized method has the following disadvantages: **a)** The TTP that generates and distributes the key for a large group is a single point of failure. **b)** The TTP is also a most attractive target for all kinds of adversaries and attacks. **c)** To allow a single party to generate the key for a whole group might not be acceptable in all cases.

The group key management protocols are typically classified in four categories: centralized group key distribution (CGKD), decentralized group key management (DGKM), distributed/contributory group key agreement (CGKA) and distributed group key distribution (DGKD) [11].
In centralized group key management, a single entity called a Trusted Third Party (TTP), such as a Key Distribution Center (KDC), is employed for distributing a secret key to group members. Normally, TTP shares a secret key with each group member. The KDC generates a group key, encrypts it with the pairwise key, and then distributes it to the corresponding group member. Centralized key management seeks to minimize storage requirements, computational power on both client and server sides, and bandwidth utilization. Hence it is easy to implement and is storage efficient for every group member, it is not efficient for the KDC to handle changes of group membership, and the major problem of single point of failure exists.

A group key agreement protocol is a key establishment method in which, a shared secret key is derived by two or more specified parties as a function of information contributed by, or associated with each of these, such that no party can predetermine the resulting value. A group key agreement protocol is contributory [1] if each party equally contributes to the key and guarantees its freshness. A group key establishment protocol is distributory [1] if there is a party (*called trusted third party*) that generates the key and then, distributes the key surely to the other parties.

The efficiency of group key agreement protocols is measured with respect to communication complexity, as well as computational complexity. Communication complexity is quantified as both the number of rounds of communication among users and the number of messages sent/received by users, while computational complexity is mostly concerned with the number of public-key cryptography operations that users have to perform. For a group key agreement protocol to be scalable, it is important that it be able to run only in a constant number of communication rounds.

Recently, an interesting classification is proposed in [12]. In their paper, the authors organize the group key management protocols for Ad hoc networks into two approaches: topology oriented approach and flat approach.
Topology-oriented approach focus on improving key computation and communication overhead and memory storage of keys. However, the topology changes frequently (eg. MANETs) caused by the mobility of the nodes. In such situations, node arrangement and synchronization within the group structure may outweigh the benefits of these group organizations.
In flat oriented approach, there is no prior organization of the group members and all group members share a common TEK. The management of this single key is centralized at a unique server or distributed among all group members. However, it suffers from the 1-affects-n problem, where a single group membership change (*join or leave*) results in a rekeying process that disturbs all group members. Moreover, most protocols in this approach need a central server. So, they are neither scalable nor fault-tolerant.

Many GKA protocols have been proposed in the literature [5], [6], [7], [8], [9], [10], most of them are derived from the two-party Deffie-Hellman key agreement protocol. In this paper, we propose a new scalable clique I based model for group key agreement, where several simultaneously keys are functional. The model is clustering based architecture, in each cluster (*formed as a ring*), only one active key is considered. As a result, each key is agreed, managed and used only by a little number of nodes, which give our model a height scalability and rapid convergence.

III. Proposition

The general idea of the proposed model consists of dividing the set of nodes composing the network on some cliques organized on several reliable rings, each node in each ring is connected to its successor and predecessor, and it can diffuse messages to all nodes in the same ring. It collaborates in each ring where it belongs for a group key agreement using Clique I protocol, and uses the associate key for local communication in the associate ring. In case of inter rings communication, the node diffuses its messages encrypted with the local key. Receiving by nodes in the border of ring (*they have double key, each one for a ring*), those last, decrypt the message with the same key by which is encrypted, and re-encrypted it for the second way with the key associated to the adjacent ring, and diffuse it for nodes on this last ring, and so on, until the messages arrive to destinations. Next sub-sections give the functional details of the proposed group key agreement model with multiple keys. Figure 1 illustrates the network architecture of the proposed multiple GKA. The colored nodes are belonging and associating to two adjacent rings, and then, they participate to the group key agreement process in the two associate rings. The rest of nodes participate only in one ring using a local key.

A. Initial formation of clusters

The initial formation of cliques (*clusters*) consists of dividing the set of nodes in the P2P wireless network into mutually disjoint cliques, but relied with some nodes which will be belonging to two neighboring clusters (*cliques*), so that

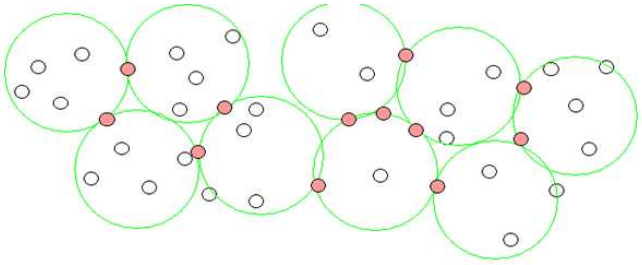

Fig. 1. Network architecture of the proposed model

all the nodes in the same clique can directly communicate with each other. Each node N_i should individually computes its view of clique C_i based on the information exchanged with its neighbors as follows: It diffuses its identity N_i to its neighboring nodes and it initializes this set $Neig_i = \{Ni\}$, and when it receives messages from node N_j containing its identity, it makes $Neig_i = Neig_i U N_j$. After stabilization, each node N_i, initializes $C_i = \{Neig_i\}$ and then sends the set $Neig_i$ to all its neighboring. When a node N_k receiving set $Neig_i$, calculates $C_k = C_k U Neig_i$. After stabilization, C_k is the final set of neighboring nodes of N_k.

B. Functional principal

Let be M_i, $\forall i \in N$ the nodes with identifier i in the same ring, where N is the node's number in this ring. A GKA protocol consists of two main phases: the initialization phase (IKA), and the auxiliary key agreement (AKA). The initialization key agreement (IKA) of our proposed model is described in algorithm 1.

Algorithm 1 : Algorithm IKA

Round i $(0 < i < n)$ (*ascending flow*)
1: M_i defines randomly a number $r_i \in Z_q^*$
2: $M_i \rightarrow M_{i+1} : \{\alpha^{\{r1*r2*...ri\}/rj}, j \in [1,i]\}, \alpha^{\{r1*r2*...ri\}}$
Round n (*descending flow*)
3: M_n defines randomly a number $r_n \in Z_q^*$
4: $M_n \rightarrow all$: $\{\alpha^{Kjn*(r1*r2*...rn)/rj}, j \in [1, n-1]\}$.

M_n is called a sponsor node, α is a previously shared parameter between all group members. K_{jn} is also a previously shared secret between the sponsor and each node j in the same ring.
For the rounds corresponding to the ascending flow of algorithm 1 (*round i*), the contributions of all the members are collected. Each member M_i receives i values: $i-1$ intermediate values (*having each one (i-1)) exhibitors*) and a cardinal value (*having i exhibitors*). M_i generates a secret value, contributes by this value and transmits i components of flow (*Messages to be transmitted*) with a cardinal value to the member M_{i+1}. For the round associated with descending flow, M_n (*called representing group*) or the sponsor distributes the result to all the members of the group (*Broadcast*). Thus, for each member M_j, a value is associated among the whole of the values diffused by the sponsor $((\alpha^{K_{jn}*(r1*r2+...*rn)/rj})$. This value is high with puissance of its contributed value (r_j) is the reverse of K_{jn} to have the secrecy of the group called the common key of group for all the members, $K_G = \alpha^{r1*r2*...*R_N}$.

After a leave's operation of a member of group or a join's operation of a new member, the key must be updated; the corresponding procedures are presented below.

C. Join and leave operations

Join Operation: The algorithm corresponding to this operation is given by the two rounds associated with ascending flow and descending flow.
When a new member M_{n+1} joined in the group, the previous sponsor M_n generates a new secrecy, the pupil with the power, transmits it to M_{n+1} (*the new member*) (*step 1 and 2 of algorithm 2*). This last generates also its secrecy and diffuses the message of flow going down to all the group members (*step 3 and 4 of algorithm 2*). The round corresponding to ascending flow is carried out through all the new members. The last carries out the phase of flow going down to make it possible to all the members of the group to recomputed the new key of the group.

Algorithm 2 : Algorithm Join

Round 1: (*The ascendant flow message of the new member*)
1: M_n randomly defines a number $r_n \in Z_q^*$
2: $M_n \rightarrow M_{n+1} : \{\alpha^{\{r1*r2*...ri\}/rj}, j \in [1,n]\}, \alpha^{\{r1*r2*...rn\}}$
Round 2: (*descending flow*)
3: M_{n+1} randomly defines a number $r_{n+1} \in Z_q^*$
4: $M_{n+1} \rightarrow All : \{\alpha^{Kjn*(r1*r2*...rn*1)/rj}, j \in [1,n]\}$.

Leave Operation: the algorithm corresponding to this operation is given by the round associated with downward flow.
In an operation type "leave", the member having the height index generates a new secrecy (*step 1 of algorithm 3*) and diffuses the message corresponding to descending flux to the remainder from the group (*step 2 of algorithm 3*) in order to allow only the members of the group to recalculate the new key of the group.

Algorithm 3 : Algorithm leave

Tour 1: (*flux descending message for member with height index*)
1: M_{h1} randomly define a number $r_h \in Z_q^*$
2: $M_{n+1} \rightarrow Remainder$: $\{\alpha^{Kjh*(r1*r2*..rh)/rj}, j \in [Reste]\}$

The operation of diffusion associated to IKA (*descending flow*) as described in clique I presents a significant cost, related to the high number of messages to be transmitted, which has a significant impact on the "scalability" of the system. However, in our proposed model, it is reduced as much as possible by reducing the simultaneously participating nodes in the same ring for the same key.

D. Inter rings communication

As described bellow, each node in a ring maintains a key calculated collaboratively with other nodes in this ring using clique 1 for example; it used it for local ring communication. Nodes belonging to two adjacent rings maintain two independent keys; each one is used in its associated ring. Figure 2 illustrates the architecture of the proposed model and the inter rings communication. Node source tends to communicate with

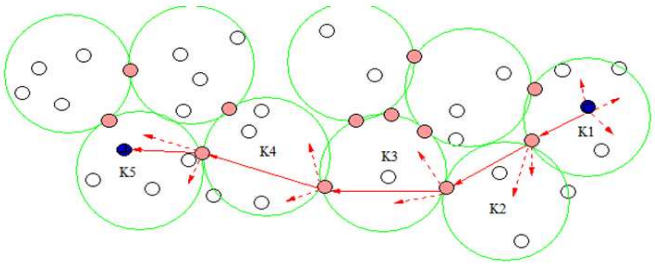

Fig. 2. Inter rings communication

another node uses its local key K1 to encrypt its message and then diffuses it. Node in the border of the same ring decrypts the message using the same key K1, encrypts it with key K2, diffuses it in the second ring, and so on, until the message arrives to destination. Algorithm 4 illustrates this process.

Algorithm 4 : Inter rings communication

1: begin
2: if (*node N_i is the initial sender*) **then**
3: Encrypt the message using the local key and diffuse it to the neigheiboring nodes
4: else *//At the reception of a message (request)*
5: Decrypt the message using its own local key
6: Encrypt it with the next ring key and forward it
7:End.

E. Fault tolerance prevention process

As described above, when a node belonging to two rings leaves the system, the network will be divided to two parts that can't communicate between them (*absence of coordinator*). To cure this problem, the coordinate nodes (*those belonging to two rings*) maintain an additional P2P links to 4 other nodes (*two nodes on each ring*). These later nodes will replace the coordinate nodes when they fails for maintaining the stabilization of system.

F. Mobility

Considering node mobility, a node moving from a cluster to another one, will be considered as a leaving node from the first cluster and a joining node for the second cluster. However, nodes in these clusters does not recalculates another key. Using node participating in two neigheiboring clusters (*relay node*), the mobile node recovers the key of its new clusters by exchange messages with relay node, messages are encrypted with the old key.

IV. Performance evaluation

Several evaluation metrics that are used to evaluate the performance of group key agreements protocols are discussed in the literature [4]. Performance of the contributory key agreement can be divided into two categories: computation cost and communication cost. Communication costs include the total number of rounds, and total number of messages (*both unicast and broadcast messages*). Computation costs consist of the total number of cryptographic signatures, total sequential exponentiations, and total number of verifications. Unlike Clique I, Our proposed model uses only a few set of nodes for key agreement. Then, it converges rapidly with low cost communication.
Considering a network with n nodes[1], for IKA establishment, Clique I needs more overhead messages (*see Figure 3*), however, in our proposed mechanism, each node communicates with few nodes to agree on a key.

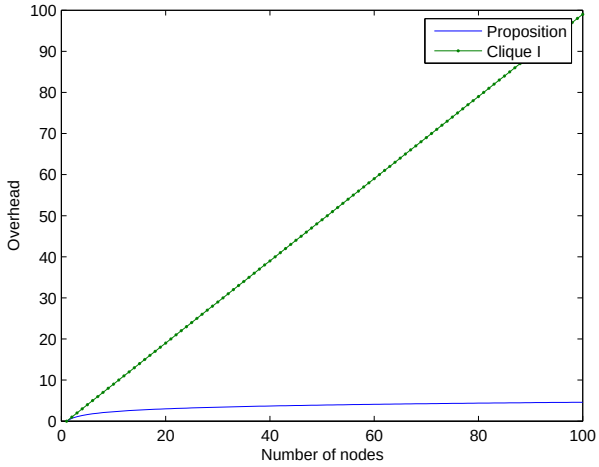

Fig. 3. Overhead for IKA

For the maintenance of the architecture and its stabilization, each node should store only a few information, just for those in the same cluster (*see Figure 4*). This is an important factor for the scalability of the system.

V. Conclusion and Future Works

In this paper, we have proposed a multi group key agreement mechanism to secure communication between nodes in P2P wireless networks. The proposed mechanism is based on a multiple keys; each one is constructed independently of others. When communication is between nodes in the same ring, they use a local key, and when the communication is inter rings, a series of encryption/decryption are down using a key associated to each ring.
The preliminary performance evaluation shows that our proposed model is more scalable. In case of join/leave operation (*where key agreement will be rebuild*), only nodes in just one

[1]Results are obtained using Matlab V7

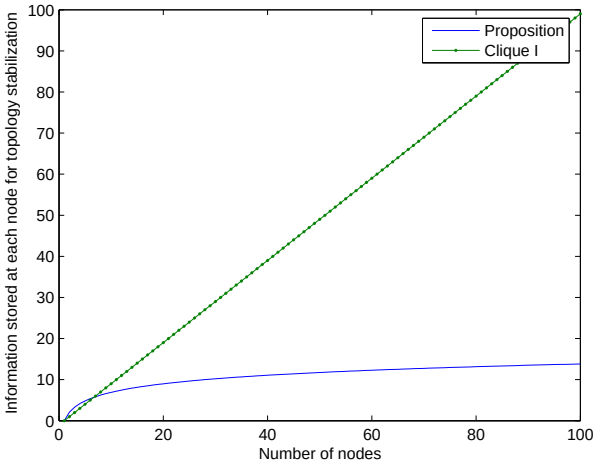

Fig. 4. Information size stored at each node

cluster will recalculate a novel key, this gives our model better fault tolerance.

In future work, we envision to experiment our model for very large network, and to evaluate the impact of mobility on the algorithm convergence.

REFERENCES

[1] R. Bhaskar, *Group Key Agreement in Ah hoc Networks*. Rapport de Recherche N 4832 INRIA, May 2003.

[2] R. Shirey, *Internet Security Glossary*, RFC 2828, 2000.

[3] J. Nam, S. Kim, D. Won and C. Jang, *Group key agreement protocols for combined Wired/Wireless networks*, The Journal of the KICS, Vol.30/No.6C, June 2005, pp.607-615.

[4] S. Zheng, D. Manz, and J. Alves-Foss, *A communication computation efficient group key algorithm for large and dynamic groups*, Technical report, University of Idaho, Sep. 2004.

[5] M. Burmester and Y. Desmedt, *A secure and efficient conference key distribution system*, Advances in Cryptology -EUROCRYPT, 1994.

[6] M. Steiner, G. Tsudik, and M. Waidner, *Key agreement in dynamic peer groups*, IEEE Transactions on Parallel and Distributed Systems, 2000.

[7] Y. Kim, A. Perrig, and G. Tsudik, *Simple and fault-tolerant key agreement for dynamic collaborative groups*, ACM CCS, 2000.

[8] E. Bresson, O. Chevassut, and D. Pointcheval, *Dynamic group Diffie Hellman key exchange under standard assumptions*, In Advances in Cryptology - EUROCRYPT, 2002.

[9] J. Katz and M. Yung, *Scalable protocols for authenticated key exchange*, Advances in Cryptology - CRYPTO, 2003.

[10] C. Boyd and J. Nieto, *Round-optimal contributory conference key agreement*, 6th International Workshop on Practice and Theory in Public Key Cryptography, 2003.

[11] S. Magliveras, W. Wei and X. Zou, *Notes on the CRTDH Group Key Agreement Protocol*, in proceedings of the 28th International Conference on Distributed Computing Systems Workshops, 2008

[12] K. Drira, H. Seba, and H. Kheddouci. *An effecient clustering scheme for group key management in manet*. IEEE Transactions on Parallel and Distributed Systems, (33) :1094-1107, 2010.

[13] Y.-M. Tseng, C.-C. Yang, D.-R. Liao, *A secure group communication protocol for ad hoc wireless networks*, in: Advances in Wireless Ad Hoc and Sensor Networks, Signals and Communication Technology Series, Springer, 2007.