A new Hierarchical Group Key Management based on Clustering Scheme for Mobile Ad Hoc Networks

Ayman EL-SAYED, IEEE Senior Member
Department of Computer Science and Engineering,
Faculty of Electronic Engineering,
Menoufiya University, Menouf 32952, Egypt.
Email: ayman.elsayed@el-eng.menofia.edu.eg

***Abstract*—The migration from wired network to wireless network has been a global trend in the past few decades because they provide anytime-anywhere networking services. The wireless networks are rapidly deployed in the future, secure wireless environment will be mandatory. As well, The mobility and scalability brought by wireless network made it possible in many applications. Among all the contemporary wireless networks,Mobile Ad hoc Networks (MANET) is one of the most important and unique applications. MANET is a collection of autonomous nodes or terminals which communicate with each other by forming a multihop radio network and maintaining connectivity in a decentralized manner. Due to the nature of unreliable wireless medium data transfer is a major problem in MANET and it lacks security and reliability of data. The most suitable solution to provide the expected level of security to these services is the provision of a key management protocol. A Key management is vital part of security. This issue is even bigger in wireless network compared to wired network. The distribution of keys in an authenticated manner is a difficult task in MANET. When a member leaves or joins the group, it needs to generate a new key to maintain forward and backward secrecy. In this paper, we propose a new group key management schemes namely a Hierarchical, Simple, Efficient and Scalable Group Key (HSESGK) based on clustering management scheme for MANETs and different other schemes are classified. Group members deduce the group key in a distributed manner.**

Keywords– Group Key management; Mobile Ad hoc network; MANET security; Unicast/Multicast protocols in MANET.

I. Introduction

Mobile Ad Hoc Network (MANET) [1], [2] is kind of mobile, multiple hops, and self-discipline system, not depend on the fixed communication facilities. Ad Hoc network is a series of nodes in structure which move anywhere at will, the network nodes distribute dynamically, nodes contact others through wireless network, every network node has the double functions as terminal and routers, the nodes are peer-to-peer, communicate with a high degree of coordination. Wireless Ad Hoc network is flexibility with a wide foreground of application, mainly used in multimedia conference, emergency rescue, relief, exploration, military action and sensor network etc. [3]. A communication session is achieved either through single-hop transmission if the recipient is within the transmission range of the source node, or by relaying through intermediate nodes otherwise. For this reason, MANETs are also called multi-hop packet radio network [4], [5]. However, the transmission range of each low-power node is limited to each other's proximity, and out-of-range nodes are routed through intermediate nodes. On the contrary to traditional network architecture, MANET does not require a fixed network infrastructure; every single node works as both a transmitter and a receiver. Nodes communicate directly with each other when they are both within the same communication range. Otherwise, they rely on their neighbors to relay messages. The self-configuring ability of nodes in MANET made it popular among critical mission applications like military use or emergency recovery. However, group key management for large and dynamic groups in MANETs is difficult problem because of the requirement of scalability, security under the restrictions of nodes' available resources and unpredictable mobility [6]. But the group key management protocols dedicated to operate in wired networks are not suited to MANET, because of the characteristics and the challenges of such environments [7]. So many researchers are interesting of group key management for MANET. In our issue, group key management means that multiple parties need to create a common secret to be used to exchange information securely. Without central trusted entity, two people that have not previously a common share key can create a key based on the Diffie-Hellman (DH) protocol [8]. DH key agreement requires that both the sender and recipient of a message have key pairs. By combining one's private key and the other party's public key, both parties can compute the same shared secret number. This number can then be converted into cryptographic keying material. It is called 2-party DH protocol that can be extended to a generalized version of n-party DH. In [9], the authors integrated the DH key exchange into the Digital Signature Algorithm (DSA) and in [10], the authors fix this integration protocols so that both forward secrecy and key freshness can be guaranteed, while preserving the basic essence of the original protocols. This fix also provides key freshness because every session key is a function of ephemeral secrets chosen by both parties, so neither party can predetermine a session key's value since he would not know what the other party's ephemeral secret is going to be. However, robust key management services are central to ensuring privacy protection in wireless ad hoc network settings. Existing approaches to key management, which often rely on trusted, centralized entities, are not well–suited for the highly dynamic, spontaneous nature of ad hoc networks. So many researchers are interesting to make proposals for key management techniques that are

surveyed in [11] to find an efficient key management for secure and reliable. This paper proposes one of the group key management schemes namely a Hierarchical, Simple, Efficient and Scalable Group Key (HSESGK) based on clustering management scheme for MANETs. Group members compute the group key in a distributed manner. This hierarchical contains two levels only, first level for all coordinators of the clusters as a main group's members; it is called cluster head (CH) that is selected by the algorithms shown in [12], [13], [14], the second level for the members in a cluster with its cluster head. Then there are two secret keys obtained in a distributed manner, the first key among all the CHs and the second key among cluster's members and its CH. HSESGK uses double trees in each cluster for robustness and avoid fault tolerance. Also group key management is to ensure scalable and efficient key delivery, taking into account the node mobility.

The remainder of this paper is organized as follows: Section II reviews related work such that MANET routing protocols for both unicast and multicast and security requirements. Also this section describes the overview of MANET key management and short note about our proposal. Details of our group key management scheme are described in Section III and our scheme is discussed with some features in Section IV. Finally, we conclude the paper in Section V.

II. Related work

A. MANET unicast routing protocols

Several routing protocols [15] have been proposed in recent years for possible deployment of Mobile Ad hoc Networks (MANETs) in military, government and commercial applications. In [16], these protocols are reviewed with a particular focus on security aspects. The protocols differ in terms of routing methodologies and the information used to make routing decisions. Four representative routing protocols are chosen for analysis and evaluation including: Ad Hoc on demand Distance Vector routing (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and Temporally Ordered Routing Algorithm (TORA). Secure ad hoc networks have to meet five security requirements: confidentiality, integrity, authentication, non-repudiation and availability. The analyses of the secure versions of the proposed protocols are discussed with respect to the above security requirements. Routing protocols for ad hoc wireless networks can be classified into three types based on the underlying routing information update mechanism employed as shown in Fig. 1. An ad hoc routing protocol could be reactive (on demand), proactive (table driven) or hybrid.

Reactive routing protocols obtain the necessary path, when required, by using a connection establishment process. Such protocols do not maintain the network topology information and they do not exchange routing information periodically. In this section, we will focus on three routing protocols and some of their secure versions. First, we discuss DSR [17]. The secure versions, such as, QoS Guided Route Discovery [18], Securing Quality of Service Route Discovery [19], Ariadne [20] and CONFIDANT [21] are presented as well. Second, AODV [22] is discussed with its secure versions, CORE [23],

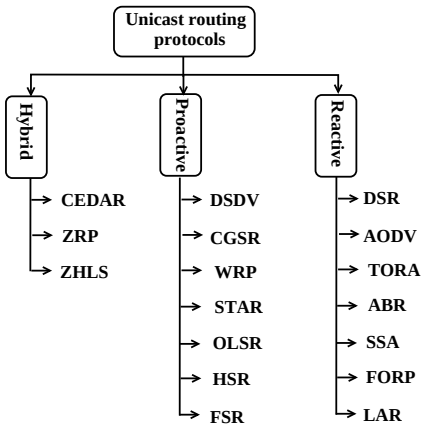


Fig. 1. Ad hoc unicast routing protocols

SAODV [24] and SAR [25]. Finally, TORA [26] is discussed followed by the discussion of two ad hoc security techniques, SPREAD [27] and ARAN [28]. We focus more on reactive routing protocols because they often outperform proactive ones due to their ability to adjust the amount of network overhead created to track the mobility in the network affecting current communication.

In ***proactive or table driven routing protocols***, such as DSDV [29] or OLSR [30], every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Routing information is generally flooded in the whole network. Whenever a node requires a path to a destination, it runs an appropriate path finding algorithm on the topology information it maintains.

Hybrid routing protocols such as ZRP [31] and SRP [32] are protocols that combine the best features for both reactive and proactive routing protocols. For example, nodes communicate with their neighbors using proactive routing protocols and communicate with far distance nodes using reactive routing protocols.

B. MANET Multicast routing protocols

There is a need for multicast traffic also in ad hoc networks. The value of multicast features with routing protocols is even more relevant in ad hoc networks, because of limited bandwidth in radio channels [33]. Some multicast protocols [34], [35] are based to form and maintain a routing tree among group of nodes. Some other are based on to use routing meshes that have more connectivity than trees etc.

The various classifications of the multicast routing protocols in MANETs are shown in Fig. 2. It illustrates the main classification dimensions for multicast routing protocols such as: *multicast topology*, *initialization approach*, *routing scheme*, and *maintenance approach*.

Multicast topology [36]: it is classified into two approaches namely mesh based and tree based [37], [38]. Tree based approach is classified into two types: *Source tree based*, in which each source creates a separated tree that contains the source as a root of the tree. *Shared tree based*, in which

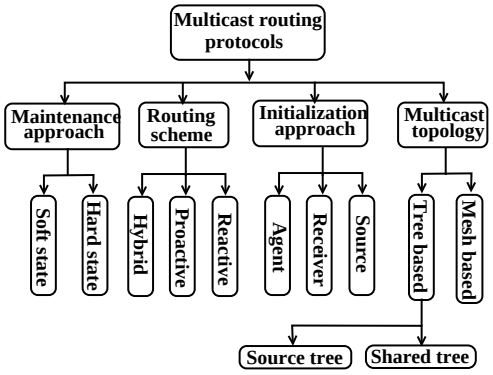


Fig. 2. Ad hoc multicast routing protocols

one tree is created in the entire network which includes all sources and receivers. Mesh based approach depends on multiple paths between any source and receivers pair. The mesh based protocols create the tree dependent on the mesh topology. These redundant paths are useful in link failure case and provide higher packet delivery ratio.

Routing initialization approach: Routing initialization is classified into three approaches namely source-initiated, receiver-initiated, and hybrid approach [39]. *Source initiated*: the source is responsible of construction and maintenance the group tasks. *Receiver initiated*: the receiver searches the multicast group to join with dedicated source. *Hybrid initiated*: the multicast group construction and maintenance tasks are done by either the source or the receiver.

Routing scheme: Routing scheme is classified into three approaches namely table-driven (proactive), on-demand (reactive), and hybrid approach [38], [39] as the same meaning in the unicast routing protocols explained in previous section.

Maintenance approach: Multicast maintenance is classified into two approaches namely soft-state and hard-state. *Soft-state approach*: a route maintenance process initiated periodically by flooding the network with control packets to explore other routes between source and receiver. This approach has the advantage of reliability and better packet delivery ratio, but it is much makes overhead over the network as it continuously floods the network with control packets [39]. *Hard-state approach*: a route maintenance process is established by two types namely reactive and proactive. In reactive approach, broken link recovery process is initiated only when a link breaks. The second type is proactive approach, in which routes are reconfigured before a link breaks, and this can be achieved by using local prediction techniques based on GPS or signal strength [39].

C. Security Requirements

The security services of ad hoc networks are not different of those of other network communication paradigms. Specifically, an effective security paradigm must ensure the following security primitives: *identity verification*, *data confidentiality*, *data integrity*, *availability*, and *access control*. Although solutions to the above concerns have been developed and widely deployed in the wired domain, the amorphous, transient properties of ad hoc networks preclude their adaptation to serverless network environments, which are often comprised of small devices. Instead, security solutions, in general, and key managements should strive for the following characteristics:

***Lightweight*:** Solutions must minimize the computation and communication processing required to ensure the security services to accommodate the limited energy and computational resources of ad hoc enabled devices.

Decentralized: Like ad hoc networks themselves, attempts to secure them must be ad hoc: they must establish security without a priori knowledge or reference to centralized, persistent entities. Instead, security paradigms must levy the cooperation of all trustworthy nodes in the network.

***Reactive*:** Ad hoc networks are dynamic: nodes trustworthy and malicious may enter and leave the network spontaneously and unannounced. Security paradigms must react to changes in network state; they must seek to detect compromises and vulnerabilities; they must be reactive, not protective.

***Fault–Tolerant*:** Wireless transfer mediums are known to be unreliable; nodes are likely to leave or be compromised without warning. The communication requirements of security solutions should be designed with such faults in mind; they mustn't rely on message delivery or ordering.

D. MANET key management overview

MANET has some constrains such its energy constrained operations, limited physical security, variable capacity links and dynamic topology. So, there are different Key Management schemes are used to achieve the high security in using and managing keys. The crucial task in MANET uses different cryptographic keys for encryption like symmetric key, asymmetric key, group key and hybrid key (i.e. mixed of both symmetric key and asymmetric key). Here we discuss about some of the important Key Management schemes in MANET and they are shown in Fig. 3.

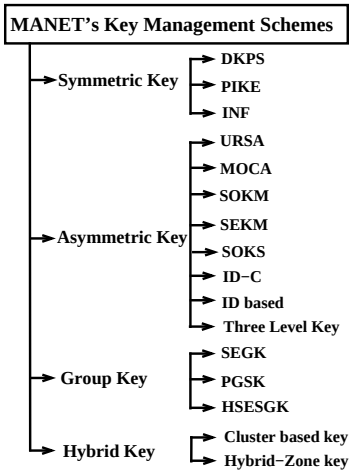


Fig. 3. Key Management Schemes in MANET

1) Symmetric Key Management: In symmetric key management, the same keys are used by sender and receiver. This key is used for encryption the data as well as for decryption the data. If n nodes wants to communicate in MANET, k number of key pairs are required, where k=n(n-1)/2. Some of the symmetric key management schemes in MANET are Distributed Key–Pre Distribution Scheme (DKPS) [40], Peer Intermediaries for Key Establishment (PIKE) [41], and Key Infection (INF) [42].

2) Asymmetric Key Management: Asymmetric keys uses two-part key. Each recipient has a private key that is kept secret and a public key that is published for everyone. The sender looks up or is sent the recipient's public key and uses it to encrypt the message. The recipient uses the private key to decrypt the message and never publishes or transmits the private key to anyone. Thus, the private key is never in transit and remains invulnerable. This system is sometimes referred to as using public keys. This reduces the risk of data loss and increases compliance management when the private keys are properly managed. Some of the asymmetric key management schemes in MANET are Self-Organized Key Management (SOKM) [43], Secure and Efficient Key Management (SEKM) [44], Private ID based Key Asymmetric Key Management Scheme [45].

3) Group Key Management Scheme: Group key in cryptography is a single key which is assigned only for one group of mobile nodes in MANET. For establishing a group key, group key is creating and distributing a secret for group members. There are specifically three categories of group key protocol. (1) Centralized, in which the controlling and rekeying of group is being done by one entity. (2) Distributed, group members or a mobile node which comes in group are equally responsible for making the group key, distribute the group key and also for rekeying the group. (3) Decentralized, more than one entity is responsible for making, distributing and rekeying the group key. Some important Group key Management schemes in MANET are Simple and Efficient Group Key Management (SEGK) [46], and Private Group Signature Key (PGSK) [47].

4) Hybrid Key Management Schemes: Hybrid or composite keys are those key which are made from the combination of two or more than two keys and it may be symmetric or a asymmetric or the combination of symmetric & asymmetric key. Some of the important Hybrid key management schemes in MANET are Cluster Based Composite Key Management [48], [49], and Zone-Based Key Management Scheme [50].

5) Our approach: In this paper, we propose the network model that contains some clusters; each cluster has its coordinator namely cluster head (Cluster initiator). The clusters are interconnected via the cluster heads. There are subgroups of members called cluster in which one member is cluster head and virtual subgroup of clusters' heads. Our model seems like Cluster-Head Gateway Switch Routing (CGSR) Protocol [51], [52] but in multicast manner, an optimized cluster based approach for multi-source multicast routing protocol in MANET [53] and Cluster Based Routing Protocol (CBRP) [54]. Our new key management scheme namely "Hierarchical, Simple, Efficient and Scalable Group Key based on clustering" (HSESGK) scheme that has main idea shown in [55]. The basic idea of our scheme is that a multicast tree is formed in MANETs for efficiency. A multiple tree based multicast routing scheme are used as mentioned in [56], [57], which exploit path diversity for robustness. Also in [46], the author used two multicast trees for improving the efficiency and maintains it in parallel fashion to achieve the fault tolerances. So, in our scheme, two multicast trees are used for each subgroup (i.e. cluster subgroups or cluster heads' subgroup). For example, in a cluster, the connection of multicast tree is maintained be its cluster head that compute and distribute the intermediate keying materials to all members in this cluster through the active tree links. Also the cluster head is responsible for maintaining the connection of the multicast subgroup. In MANET, main cluster head (MANET initiator) has the same role of cluster head, but on the clusters' subgroup.

III. Our Group key management scheme

A. Notations and assumptions

Firstly, every node takes a valid certificate from offline configuration before entering the network. An underlying public key infrastructure is then used to manage certificates. However, many researchers are interesting of this hot topic, and most key management proposals suffer the man-in-the-middle attack. In this paper, each member has a unique identifier and all keying materials signed by the coordinator (i.e. cluster head) in subgroup to make sure authenticity and integrity, in order to avoid the man-in-the-middle attack. Also, a group member has a password to join or can present a valid certificate. In our work, a group member can join by using a valid certificate. Here, for simplicity, we assume that a node can join a group if it has a valid certificate. Some notations used in HSESGK are listed as follows:

$\boldsymbol{M}_i$	i^{th} group member.
$\boldsymbol{g}$	Exponentiation base.
$\boldsymbol{p}$	Prime value.
$\boldsymbol{CH}_i$	i^{th} Cluster Head.
$\boldsymbol{MCH}$	Main Cluster Head.
$\boldsymbol{N}$	Total number of group members.
$\boldsymbol{N}_c$	Total number of Clusters.
$\boldsymbol{n}_{ci}$	Number of group members in i^{th} Cluster.
$\boldsymbol{r}_i$	A random number generated by i^{th} member, also called member private key.
$\boldsymbol{br}_i$	Blinded i^{th} member key. $\boldsymbol{br}_i = \boldsymbol{(g)}^{ri} \boldsymbol{\ mod\ p}$
$\boldsymbol{k}_i$	Internal i^{th} member key, or intermediate key.$\boldsymbol{k}_i = \boldsymbol{(b}_{ri}\boldsymbol{)}^{ki} \boldsymbol{\ mod\ p}$
$\boldsymbol{bk}_i$	Blinded internal i^{th} member key, or blinded intermediate key. $\boldsymbol{bk}_i = \boldsymbol{(g)}^{ki}$
$\boldsymbol{K}_{Gci}$	A key of i^{th} Cluster. $\mathbf{K}_{Gci}=(\mathbf{br}_{io})^{knci} \mathbf{mod\ p}$
$\boldsymbol{K}_G$	A key among CHs. $\mathbf{K}_G=(\mathbf{br}_{co})^{kNc} \mathbf{mod\ p}$
$\boldsymbol{h(m)}$	The digest of m

B. Overview of HSESGK

We proposed a new approach which aims to address the scalability problem while taking into consideration the dynamic aspect of the group members and dynamicity of nodes

in MANET. There are two trees on the network to avoid the robustness problem as well. Our approach is based on clustering manner. Each cluster is initiated by Cluster Head (CH), namely cluster initiator or coordinator initiator. Cluster head has then two keys; one for its cluster subgroup and another one for the interconnection among the clusters via cluster heads. Firstly, we describe our network model that is the mobile ad hoc network based on clustering that contains for example five clusters as shown in Fig. 4. There is a cluster head for each cluster and one of the cluster heads is MANET initiator or Main Cluster Head (MCH).

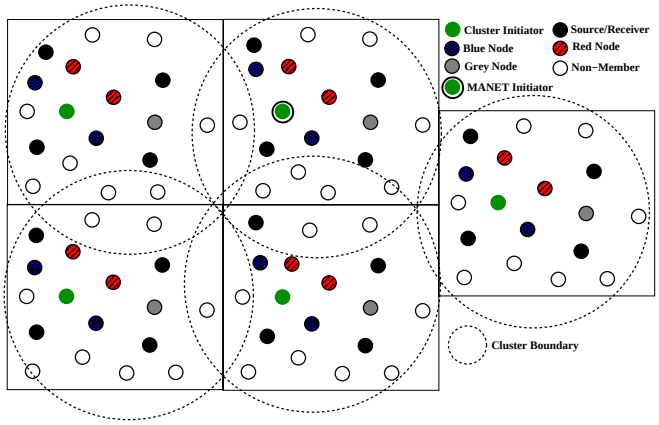


Fig. 4. MANET based on clustering.

There are many multicast routing protocols have been proposed, these protocols are classified as shown before in section 2.2. We proposed another one in the category of multicast topology, tree-based and shared tree with double trees, namely Blue tree and Red tree. All clusters then works in parallel to construct two trees. Logically, a group member views the two trees as identical trees. The group members have to be in both multicast trees.

1) Inside the Cluster: In a cluster, the cluster head (Cluster initiator) starts to initialize the process for a cluster multicast subgroup by broadcasting a join advertises message across the entire cluster. This cluster is bounded and having a fixed diameter. Each node is associated with three colors (blue, red, and grey). A node will choose its color (grey) when its total number of neighbors is less than a predefined threshold value (depending on average node degree, for instance, half of its degree). Other nodes randomly choose blue or red as their color with probability equal to 0.5. For the first received message, a grey node stores the upstream node ID and rebroadcasts the message except the node that the message is coming from. For a non-grey node, it stores the upstream node ID and rebroadcasts the message only if the upstream node is the same color, a sender/receiver, or a grey node. Based on the join response back from group members to the cluster head, two multicast trees are formed in parallel, as shown in Fig. 5. It is noted that both trees consist of group members and intermediate non-member nodes. Sure both tree are constructed in parallel and in distributer processing manner, but in blue tree‘s point of view, we find that the red’s nodes stop the broadcasting for blue tree and just blue’s nodes who broadcasting the join advertises to both blue’s nodes and grey nodes as shown in Fig. 6. As well, in red tree’s point of view, we find that the blue’s nodes stop the broadcasting for red tree and just red’s nodes who broadcasting the join advertises to both red’s nodes and grey nodes as shown in Fig. 7.

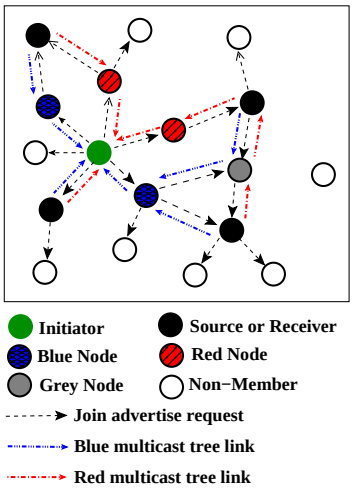


Fig. 5. Double multicast (Blue and Red) trees structure for a cluster

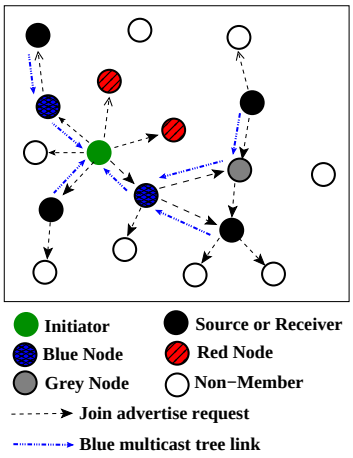


Fig. 6. Blue trees point of view for constructing itself.

2) Interconnection among the Clusters: The interconnection among the clusters is via the main cluster head (MANET initiator) starts to initialize the process for a cluster heads’ multicast subgroup by broadcasting a join advertises message across the entire MANET. We supposed the nodes no change its color, blue node still blue, red node still red, grey node still grey, and another cluster heads are source/receiver, viz, the cluster heads seems as a virtual cluster. So we can apply the same scenario that is used before in the cluster, to get both blue and red multicast trees among all cluster heads in MANET. This join advertises are broadcast across the entire

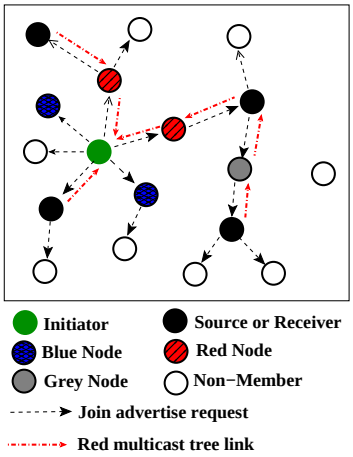


Fig. 7. Red trees point of view for constructing itself.

network as shown in Fig. 8, in which the sequence number is used to avoid the loop, and the number of hops. Based on the join response back from cluster heads to the main cluster head, two multicast trees are formed in parallel, as shown in Fig. 8. The double multicast trees among cluster heads are created and are shown in Fig. 9. Both trees consist of cluster heads, some of group members, and intermediate non-group member nodes. The resultant two trees could be disjoint or may share a common node.

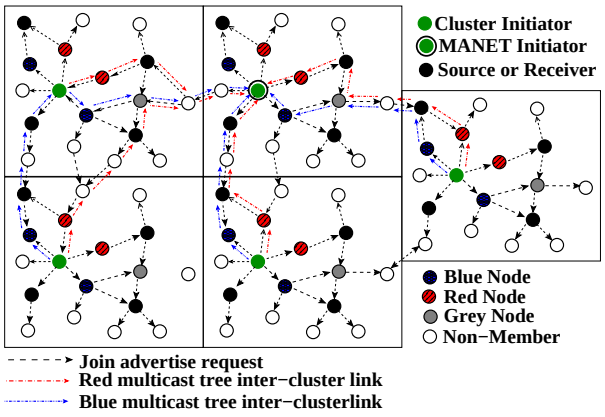


Fig. 8. Double multicast (Blue and Red) trees structure among cluster heads

As well, the double trees among cluster heads could be disjoint or may share some links in the double trees in the clusters. It is clear from the Fig. 10. Thus a dynamic double multicast trees structure for both all clusters and the subgroup of cluster heads is constructed as shown in Fig. 10. Initially the main cluster head is responsible for sending the refreshment message periodically to maintain the connection of the double trees structure. After a predefined period of time, a member could decide to act a cluster head and notify the cluster members that it is on duty to maintain the cluster subgroup. As well, a cluster head could decide to act a main cluster head

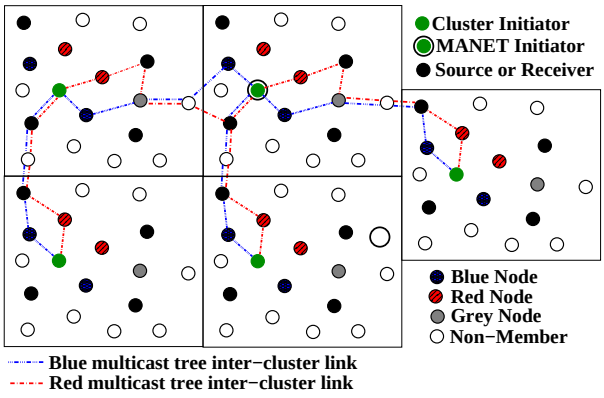


Fig. 9. Cluster Heads' multicast (Blue and Red) trees structure

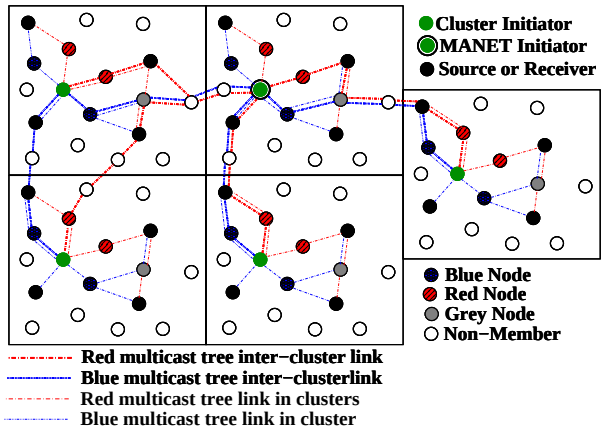


Fig. 10. Double multicast (Blue and Red) trees structure among all members in MANET

and notify the cluster heads that it is on duty to maintain the MANET group.

C. Multicast group mangement

1) A new member joins: A new member want to join a group, it could broadcast join requests to the group. The new member becomes a legitimate group member once its request is approved by any existing group member or by the cluster head of this group member. Any existing member can send replies back and send alarm "*new member*" to its cluster head. This cluster head then does the same procedure of handling join request that is similar to the above subgroup advertisement to ensure the consistency of the double multicast tree structure.

2) A member leaves: The processing of handling members who leave is more complicated than handling the joining of new members. A leaving member will not send a leaving notice. It leaves the group silently. Even if it could send a message and notify its leaving, this notice could get lost in a dynamic environment. There are a physical leaving and a logical leaving. For the physical leaving, a node moves out the range of the network or it switches its transmitter off. For a logical leaving, a node still stays inside the network, but

it does not participate in the group activity. So there are two scenarios, as follows:

First scenario: depends on detecting leaved members by its neighbors. The members are classified based in its places as follow:

1) A member is in the cluster double trees only, the neighbor of leaved member detect the leaved member and informs cluster head of its cluster to refresh the double multicast trees in this cluster.
2) A member is in cluster heads' double trees only, one of neighbor detects the leaving a member, then inform the main cluster head to refresh the double trees.
3) A member is in both a cluster double tree and cluster heads' double trees, a neighbor of leaved member detects that there is a member leaved, and inform both the main cluster head and its cluster head to refresh the double multicast trees of both cluster heads subgroup and the cluster of leaved member.

Second scenario: is based on a "*member refresh*" message that is periodically broadcasted by the cluster head across the subgroup. Each member should send an "*ack*" message back to indicate its status. The cluster head will determine whether a member remains attached or has left based on its response status within a certain time. If the cluster member on duty haven't receive "*member refresh*" message from its cluster head within a certain time, it sends a message "I am a cluster head" and send refresh the double trees in the cluster, at the same time the main cluster head detects one cluster head leaved, so it refresh the double trees of cluster heads' subgroup and so on for the main cluster head, if it leaves. This scenario is quite more costly than the first scenario but is more appropriate for a highly dynamic network like MANET where the nodes move frequently and cause the connection to be broken frequently.

D. Group key establishment protocol

The idea of subgroup key agreement protocol is that all subgroup members maintain a logic key's tree in local storage space. This key's tree is used to deduce the final common subgroup key. Our scheme is based on key's tree structure, for each subgroup; there is individual key's tree and a common subgroup key. The key's tree structure (e.g. with four members included the cluster head member, as an example) in our scheme is shown in Fig. 11.

Each member generates a private number; r_1, r_2, r_3, and r_4 for the members M_1, M_2, M_3, and M_4 respectively. The cluster head of a subgroup generates the numbers r and r_0, and informs all other members in its subgroup.The two numbers (r, r_0) at the two ends of the key tree for efficient group key refreshing and the cluster head role switching. Also, it is responsible for handling the member join and leave. All members reply its cluster head by intermediate keys to calculating keys. In this example: a subgroup contains four nodes. The cluster head multicast the intermediated blind keys to all members. So, each member deduces locally the final common subgroup key. The given parameters' value for each node: g=2, p = 13, r=3 then br = g^r mod p = 2^3 mod 13 = 8,

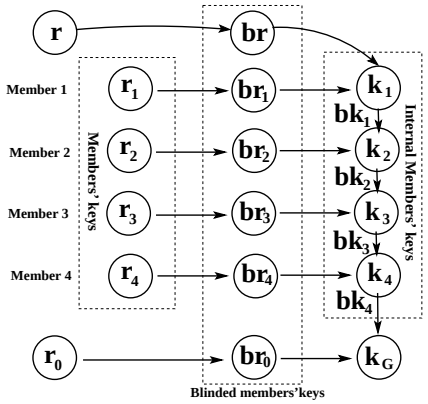


Fig. 11. Key's tree structure to generate group key (K_G) with 4 members

r_0 =5 then $br_0 = g^{r_0}$ mod p = 2^5 mod 13 = 6. Each member i, $\forall i \epsilon [1,4]$, can calculate the K_G as follows:

Inside M_1
r_1 = 4, $br_1 = g^{r_1}$ mod p = 2^4 mod 13= 3,
$k_1 = {br_1}^r$ mod p= 3^3 mod 13 =1,
$bk_1 = g^{k_1} = 2^1$ =2
$\Longrightarrow k_1 = {br}^{r_1}$ **mod p** = 8^4 **mod 13 = 1**
$\Longrightarrow k_2 = {br_2}^{k_1}$ mod p = 6^1 mod 13 = 6
$\Longrightarrow k_3 = {br_3}^{k_2}$ mod p = 11^6 mod 13 = 12
$\Longrightarrow k_4 = {br_4}^{k_3}$ mod p = 12^{12} mod 13 = 1
$\Longrightarrow K_G = {br_0}^{k_4}$ **mod p** = 6^1 **mod 13 = 6**

Inside M_2
r_2 = 5, $br_2 = g^{r_2}$ mod p = 2^5 mod 13= 6,
$k_2 = {br_2}^{k_1}$ mod p= 6^1 mod 13 =6,
$bk_2 = g^{k_2} = 2^6$ =64
$\Longrightarrow k_2 = {bk_1}^{r_2}$ **mod p** = 2^5 **mod 13 = 6**
$\Longrightarrow k_3 = {br_3}^{k_2}$ mod p = 11^6 mod 13 = 12
$\Longrightarrow k_4 = {br_4}^{k_3}$ mod p = 12^{12} mod 13 = 1
$\Longrightarrow K_G = {br_0}^{k_4}$ **mod p** = 6^1 **mod 13 = 6**

Inside M_3
r_3 = 7, $br_3 = g^{r_3}$ mod p = 2^7 mod 13= 11,
$k_3 = {br_3}^{k_2}$ mod p= 11^6 mod 13 =12,
$bk_3 = g^{k_3} = 2^{12}$ =4096
$\Longrightarrow k_3 = {bk_2}^{r_3}$ **mod p** = 64^7 **mod 13 = 12**
$\Longrightarrow k_4 = {br_4}^{k_3}$ mod p = 12^{12} mod 13 = 1
$\Longrightarrow K_G = {br_0}^{k_4}$ **mod p** = 6^1 **mod 13 = 6**

Inside M_4
r_4 = 6, $br_4 = g^{r_4}$ mod p = 2^6 mod 13= 12,
$k_4 = {br_4}^{k_3}$ mod p= 12^{12} mod 13 =1,
$bk_4 = g^{k_4} = 2^1$ =2
$\Longrightarrow k_4 = {bk_4}^{r_4}$ **mod p** = 12^{12} **mod 13 = 1**
$\Longrightarrow K_G = {br_0}^{k_4}$ **mod p** = 6^1 **mod 13 = 6**

1) Initialization: CH announces its role and broadcasts two random keys (r, r_0) and its br_c, br, and br_0. Each member has unique identifier (ID) that is given by its cluster head when joining the group. At the initialization phase, the members are sorted by their ID. M_i, $\forall$ i ϵ [1,N_c], (where N_c is number of subgroup's members) generates a private random number r_i then compute the br_i and send it to its CH. CH is then responsible for computing $k_1 \ldots k_{N_C}$ and $bk_1 \ldots bk_{N_c}$ and

then multicasts them to the subgroup's members.

All keying materials are put in one package and the order of blinded intermediate key materials shows the structure of the key tree. Each member can thus deduce the common subgroup key (K_G). The time diagram of initialization process to deduce the common group key (K_G) in a subgroup is shown in Fig. 12 for each cluster(i.e.either members' clusters or CH's cluster).

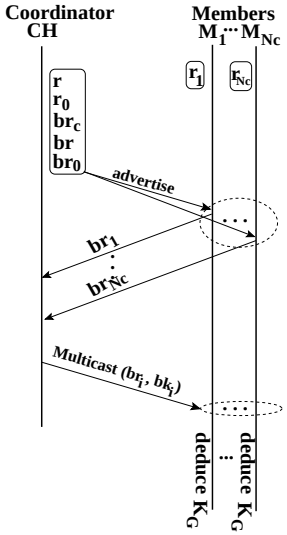
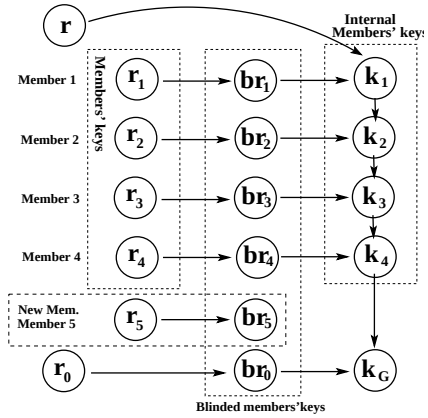


Fig. 12. Time diagram of initialization process of deducing group key (K_G) in a subgroup

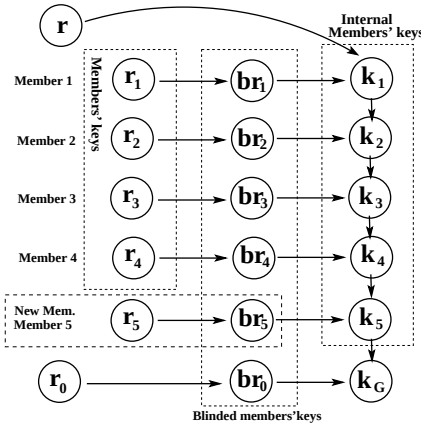
2) Member join: A new member can be easily added into the nearest cluster as described before in section III-C1. The double trees are constructed. The cluster head insert the new member in the current rightmost position and give it an ID. The cluster head does not generate any random key but still provides key independence. Given blinded keys, the new member deduce the new common subgroup key, however it cannot deduce the previous common subgroup key.

Fig. 13 depicts Key tree structure to generate group key (K_G), while a new member wants to join a subgroup. We take the same example used before in this section with adding a new member M_5. The given parameters' value for each member: g=2, p = 13, r=3 then br = g^r mod p = 2^3 mod 13 = 8, r_0 =5 then $br_0 = g^{r_0}$ mod p = 2^5 mod 13 = 6. Each member i, $\forall$ i ϵ [1, 5], can calculate the K_G as follows:

Inside M_1
r_1 = 4, $br_1 = g^{r_1}$ mod p = 2^4 mod 13= 3,
$k_1 = {br_1}^r$ mod p= 3^3 mod 13 =1,
$bk_1 = g^{k_1} = 2^1$ =2
$\Longrightarrow k_1 = {br}^{r_1}$ **mod p** = 8^4 **mod 13 = 1**
$\Longrightarrow k_2 = {br_2}^{k_1}$ mod p = 6^1 mod 13 = 6
$\Longrightarrow k_3 = {br_3}^{k_2}$ mod p = 11^6 mod 13 = 12
$\Longrightarrow k_4 = {br_4}^{k_3}$ mod p = 12^{12} mod 13 = 1
$\Longrightarrow k_5 = {br_5}^{k_4}$ mod P = 3^1 mod 13 = 3
$\Longrightarrow K_G = {br_0}^{k_5}$ **mod p** = 6^3 **mod 13 = 8**



(a) Before joining a member 5



(b) After joining a member 5

Fig. 13. Key tree structure to generate group key (K_G), while a member join a subgroup

Inside M_2
r_2 = 5, $br_2 = g^{r_2}$ mod p = 2^5 mod 13= 6,
$k_2 = {br_2}^{k_1}$ mod p= 6^1 mod 13 =6,
$bk_2 = g^{k_2} = 2^6$ =64
$\Longrightarrow k_2 = {bk_1}^{r_2}$ **mod p** = 2^5 **mod 13 = 6**
$\Longrightarrow k_3 = {br_3}^{k_2}$ mod p = 11^6 mod 13 = 12
$\Longrightarrow k_4 = {br_4}^{k_3}$ mod p = 12^{12} mod 13 = 1
$\Longrightarrow k_5 = {br_5}^{k_4}$ mod P = 3^1 mod 13 = 3
$\Longrightarrow K_G = {br_0}^{k_5}$ **mod p** = 6^3 **mod 13 = 8**

Inside M_3
r_3 = 7, $br_3 = g^{r_3}$ mod p = 2^7 mod 13= 11,
$k_3 = {br_3}^{k_2}$ mod p= 11^6 mod 13 =12,
$bk_3 = g^{k_3} = 2^{12}$ =4096
$\Longrightarrow k_3 = {bk_2}^{r_3}$ **mod p** = 64^7 **mod 13 = 12**
$\Longrightarrow k_4 = {br_4}^{k_3}$ mod p = 12^{12} mod 13 = 1
$\Longrightarrow k_5 = {br_5}^{k_4}$ mod P = 3^1 mod 13 = 3
$\Longrightarrow K_G = {br_0}^{k_5}$ **mod p** = 6^3 **mod 13 = 8**

Inside M_4
r_4 = 6, br_4= g^{r_4} mod p = 2^6 mod 13= 12,
k_4 = ${br_4}^{k_3}$ mod p= 12^{12} mod 13 =1,
bk_4 = g^{k_4} = 2^1 =2
$\Longrightarrow$ k_4 = ${bk_3}^{r_4}$ **mod p** = 4096^6 **mod 13 = 1**
$\Longrightarrow$ k_5 = ${br_5}^{k_4}$ mod P = 3^1 mod 13 = 3
$\Longrightarrow$ K_G = ${br_0}^{k_5}$ **mod p** = 6^3 **mod 13 = 8**

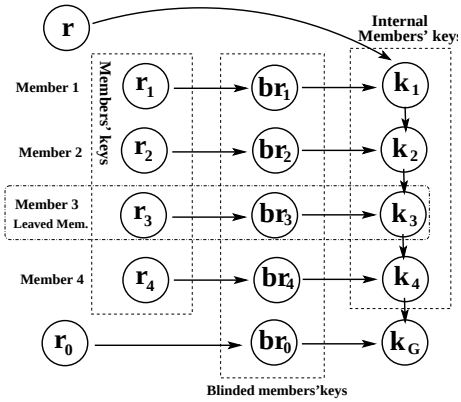
Inside M_5
r_5 = 4, br_5= g^{r_4} mod p = 2^4 mod 13= 3,
k_5 = ${br_5}^{k_3}$ mod p= 3^1 mod 13 =3,
bk_5 = g^{k_5} = 2^3 =8
$\Longrightarrow$ k_5 = ${bk_4}^{r_5}$ **mod P** = 2^4 **mod 13 = 3**
$\Longrightarrow$ K_G = ${br_0}^{k_5}$ **mod p** = 6^3 **mod 13 = 8**

3) Member leave: A member can be easily leaved from its cluster as described before in section III-C2. The double trees are constructed. It is possible that the leaved member is either a member in a cluster (subgroup) or a cluster head. *Case 1*: leaving of a member in a cluster, its cluster head generates a new random key r' instead of r and multicast the blinded value br' as well as other intermediate blinded keys. Each member i, $\forall$ i ϵ [1, N_c]\{leaved member}, can then calculate the K_{G_c}. *Case 2*: leaving of cluster head, a cluster member on duty acts as a cluster head as before, moreover, the main cluster head detects a cluster head leaved, so the leaved process seems like two leaved members (but really one leaved member), one from a cluster's subgroup and another from the cluster heads' subgroup. In two cases, the leaved process simply takes place in a subgroup as shown in Fig. 14, that depicts key tree structure to generate both group key (K_{G_c}) for the cluster of leaved member and group key (K_G) for cluster heads' subgroup via the same process, while a member leaves the multicast group.

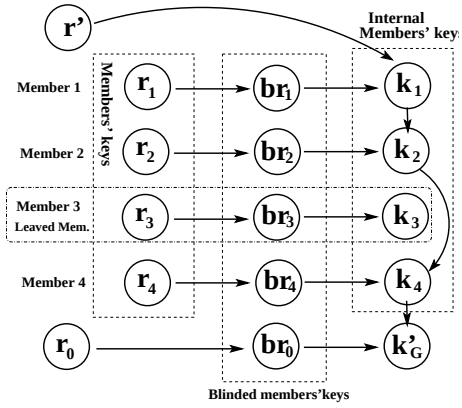
Also, we take the same example used before in this section with leaving a member M_3 in *Case 1*. The given parameters' value for each member: g=2, p = 13, r'=5 then br' = $g^{r'}$ mod p = 2^5 mod 13 = 6, r_0 =5 then br_0 = g^{r_0} mod p = 2^5 mod 13 = 6. Each member i, $\forall$ i ϵ [1, 5]\{3}, can calculate the K_G as follows:

Inside M_1
r_1 = 4, br_1= g^{r_1} mod p = 2^4 mod 13= 3,
k_1 = ${br_1}^{r}$ mod p= 3^5 mod 13 =9,
bk_1 = g^{k_1} = 2^9 =512
$\Longrightarrow$ k_1 = ${br'}^{r_1}$ **mod p** = 6^4 **mod 13 = 9**
$\Longrightarrow$ k_2 = ${br_2}^{k_1}$ mod p= 6^9 mod 13 = 5
$\Longrightarrow$ k_4 = ${br_4}^{k_2}$ mod p= 12^5 mod 13 = 12
$\Longrightarrow$ K_G = ${br_0}^{k_4}$ **mod p**= 6^{12} **mod 13 = 1**

Inside M_2
r_2 = 5, br_2= g^{r_2} mod p = 2^5 mod 13= 6,
k_2 = ${br_2}^{k_1}$ mod p= 6^9 mod 13 =5,
bk_2 = g^{k_2} = 2^5 =32
$\Longrightarrow$ k_2 = ${bk_1}^{r_2}$ **mod p**= 512^5 **mod 13 = 5**
$\Longrightarrow$ k_4 = ${br_4}^{k_2}$ mod p= 12^5 mod 13 = 12
$\Longrightarrow$ K_G = ${br_0}^{k_4}$ **mod p**= 6^{12} **mod 13 = 1**



(a) Before leaving a member 3



(b) After leaving a member 3

Fig. 14. Key tree structure to generate group key (K_G), while a member leaves the member group

Inside M_4
r_4 = 6, br_4= g^{r_4} mod p = 2^6 mod 13= 12,
k_4 = ${br_4}^{k_2}$ mod p= 12^5 mod 13 =12,
bk_4 = g^{k_4} = 2^{12} =4096
$\Longrightarrow$ k_4 = ${bk_2}^{4_4}$ mod p= 32^6 mod 13 = 12
$\Longrightarrow$ K_G = ${br_0}^{k_4}$ **mod p**= 6^{12} **mod 13 = 1**

4) Group key refresh/reinforce: The group key may need to be changed periodically, and may not be related to any change of group membership. The purpose of refreshing the group key periodically is to prevent the long time use of group keys which could be compromised. This process can be implicitly done during the switch of cluster head, or explicitly performed by the cluster head which generates a new random key r" and multicasts the blinded value br" as well as other intermediate blinded keys. Then each member i, $\forall$ i ϵ [1, N_c], can calculate the K_{G_c} as described in section III-D1. Refresh/reinforce process take place independently in each cluster, as well in the cluster heads' subgroup. That decreases the traffic control overheads and increases the scalability in MANET.

IV. Discussion

The goal of all these protocols include such as minimal control overhead, minimal processing overhead, multi-hop routing

capability, dynamic topology maintenance, loop prevention, or more secure. However many multicast routing protocols don't perform well in MANETs because in a highly dynamic environment, node move arbitrarily, and man-in-middle problem. Our paper focuses on the key management schemes that are important part of the security. So key management is an essential cryptographic primitive upon which other security primitives such as privacy, authenticity and integrity are built. As well, it has to be satisfied some features such as *Security*, *Reliability*, *Scalability*, *Robustness*, and *power consumption*, as follows:

Security: intrusion tolerance means system security should not succumb to a single, or a few, compromised nodes. So, the key management schemes should ensure no unauthorized node receives key material that can later be used to prove status of a legitimate member of the network. Here the key is computed in distributed manner, and the member provides a trusted group communication. Other issues are trust management, vulnerability. Also, proper key lengths and cryptographic algorithms of adequate strength are assumed.

Reliability: depends on the key distribution, storage and maintenance and make sure that keys are properly distributed among the nodes, safely stored where intruders aren't able to hack the keys and should be properly maintained. In our proposed, each member can deduce the common group key depending on a private value, not be exchanged and some common parameters shared among members. It means that no need to exchange the group key, so this group key is stored locally on a member with a certain security manner.

Scalability: the key management operations should finish in a timely manner despite a varying number of nodes and node densit ies. It makes use the occupied network bandwidth of network management traffic as low as possible to increase nodes' density. Making use of clustering scheme, decreases the control overhead traffic due to the double trees creation, and increase the number of members in the MANET with lowest control overhead.

Robustness: the key management system should survive despite Denial-of-Service (DoS) attacks and unavailable nodes. Because of dynamicity of the group members, necessary key management operation should execute in a timely manner, in order not to make a isolated partition in the network. In our proposal, multiple trees are used for the robustness and avoid fault tolerance.

Power consumption: Energy saving, despite recent advances in extending battery life, is still an important issue. Basically, MANETs protocols must be aware that a mobile node has a finite battery capacity. In another side, decreases the processing time, as low as possible to increase the life time of nodes. We believe that delay and delay jitter should be given the highest priority when dealing with for example video traffic over the wireless network. It means that many researchers have focused and emphasized on saving power of the node battery to last for longer time without recharging as mentioned in [58].

V. Conclusion

MANET is one of the most important and unique applications. Due to the nature of unreliable wireless medium data transfer is a major problem in MANET and it lacks security and reliability of data. A Key management is vital part of security. Key management protocols then play a key role in any secure group communication architecture. Moreover in MANET, members can join and leave the group dynamically during the whole session, plus the nodes movement. So, the key management is an important challenge because of its dynamism that affects considerably its performance. In this paper, we have studied the different key management schemes for MANET and proposed a new scheme namely HSESGK, which is an efficient/scalable hierarchical key management scheme for MANET multicast. In our scheme, the group members deduce the group key in a distributed manner. This hierarchical contains two levels only, first level for all clusters' heads as a main group's members; the second level for all clusters' members. Then there is a secret key obtained in a distributed manner for each cluster subgroup, and another secret key for clusters' heads subgroup. It is shown that our scheme reduces significantly the overall security overhead of member's join or leave compared to all other schemes and more reducing the ratio between control overheads and data. it is satisfied for some features such as Security, Reliability, Scalability, Robustness, and power consumption.

References

[1] M. Younis and S. Z. Ozer, "Wireless ad hoc networks: technologies and challenges," *Wireless Communications and Mobile Computing*, vol. 6, no. 7, pp. 889–892, 2006.

[2] S. Guo and O. W. W. Yang, "Energy-aware multicasting in wireless ad hoc networks: A survey and discussion," *Computer Communications*, vol. 30, no. 9, pp. 2129–2148, 2007.

[3] J. Wang, C. Wang, and Q. Wu, Eds., *Ad Hoc Mobile Wireless Network*. Beijing, National defense industry press, 2004.

[4] C. Xiao and W. Jie, "Multicasting techniques in mobile ad hoc networks," in *The handbook of ad hoc wireless networks*, I. Mohammad and C. D. Richard, Eds. CRC Press, Inc., 2003, pp. 25–40, 989714.

[5] L. Junhai, Y. Danxia, and . all, "Research on routing security in manet," *Application Research of Computers*, vol. 25, no. 1, pp. 243–245, 2008.

[6] R. A. and K. C. Shet, "Hierarchical approach for key management in mobile ad hoc networks," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 5, no. 1, pp. 87–95, 2009.

[7] M.-S. Bouassida, I. Chrisment, and O. Festor, "Group key management in manets," *International Journal of Network Security (IJNS)*, vol. 6, no. 1, pp. 67–79, 2008.

[8] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[9] L. Harn, M. Mehta, and H. Wen-Jung, "Integrating diffie-hellman key exchange into the digital signature algorithm (dsa)," *Communications Letters, IEEE*, vol. 8, no. 3, pp. 198–200, 2004.

[10] R. C. W. Phan, "Fixing the integrated diffie-hellman-dsa key exchange protocol," *Communications Letters, IEEE*, vol. 9, no. 6, pp. 570–572, 2005.

[11] M. Francis, M. Sangeetha, and A. Sabari, "A survey of key management technique for secure and reliable data transmission in manet," *International Journal of Advanced Research in Computer Science and Software Engineering (IJAARCSSE)*, vol. 3, no. 1, pp. 22–27, 2013.

[12] K. Hussain, A. H. Abdullah, S. Iqbal, K. Awan, and F. Ahsan, "Efficient cluster head selection algorithm for manet," *Journal of Computer Networks and Communications*, vol. 2013, no. 7, pp. 1–7, 2013.

[13] P. Sivaprakasam and R. Gunavathi, "An efficient clusterhead election algorithm based on maximum weight for manet," in *Advanced Computing (ICoAC), 2011 Third International Conference on*, Dec 2011, pp. 315–320.

[14] S. Mehta, P. Sharma, and K. Kotecha, "A survey on various cluster head election algorithms for manet," in *Engineering (NUiCONE), 2011 Nirma University International Conference on*, Dec 2011, pp. 1–6.

[15] D. Hongmei, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine, IEEE*, vol. 40, no. 10, pp. 70–75, 2002.

[16] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile ad hoc routing protocols," *Communications Surveys & Tutorials, IEEE*, vol. 10, no. 4, pp. 78–93, 2008.

[17] D. B. Johnsort, "Routing in ad hoc networks of mobile hosts," in *Mobile Computing Systems and Applications, 1994. WMCSA 1994. First Workshop on*, 1994, pp. 158–163.

[18] L. Wenjing, L. Wei, and F. Yuguang, "Spread: enhancing data confidentiality in mobile ad hoc networks," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 4, 2004, pp. 2404–2413 vol.4.

[19] R. Hauser, M. Consulting, T. Przygienda, and G. Tsudik, "Lowering security overhead in link state routing," *Computer Networks*, vol. 31, no. 8, pp. 885–894, 1999.

[20] H. Yih-Chun, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3, 2003, pp. 1976–1986 vol.3.

[21] B. Sonja and B. Jean-Yves Le, "Performance analysis of the confidant protocol," 2002, 513828 226-236.

[22] V. D. Park and M. S. Corson, "A highly adaptive distributed routing algorithm for mobile wireless networks," in *INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Driving the Information Revolution., Proceedings IEEE*, vol. 3, 1997, pp. 1405–1413 vol.3.

[23] M. Sergio, T. J. Giuli, L. Kevin, and B. Mary, "Mitigating routing misbehavior in mobile ad hoc networks," 2000, 345955 255-265.

[24] J. J. Garcia-Luna-Aceves and M. Spohn, "Source-tree routing in wireless networks," in *Network Protocols, 1999. (ICNP '99) Proceedings. Seventh International Conference on*, 1999, pp. 273–282.

[25] W. Yong, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *Communications Surveys & Tutorials, IEEE*, vol. 8, no. 2, pp. 2–23, 2006.

[26] P. Papadimitratos and Z. J. Haas, "Secure routing: Secure data transmission in mobile ad hoc networks," in *ACM Workshop on Wireless Security (WiSe 2003)*, vol. 1-58113-585-8/02/0009, San Diego, California, USA, 2003, pp. 41–50.

[27] L. Lilien, "Developing pervasive trust paradigm for authentication and authorization," in *Cracow Grid Workshop*. Institute of Computer Science, AGH University of Science and Technology, Cracow,Poland: Academic Computer Centre CYFRONET AGH, 2004, pp. 42–49.

[28] P. Jacquet, P. Muhlethaler, and A. Qayyum, "Optimized link state routing protocol," in *RFC 3626*, 2003.

[29] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA '99. Second IEEE Workshop on*, 1999, pp. 90–100.

[30] T. H. Clausen, G. Hansen, L. Christensen, and G. Behrmann, "The optimized link state routing protocol evaluation through experiments and simulation," in *In Proceedings of the IEEE Symposium on Wireless Personal Mobile Communications*, Mindpass Center for Distributed Systems, Aalborg University, Fredrik Bajers Vej 7E, DK-9220 Aalborg, Denmark, 2001.

[31] Z. Manel Guerrero, "Secure ad hoc on-demand distance vector routing," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 6, no. 3, pp. 106–107, 2002, 581312.

[32] H. Yih-Chun and B. J. David, "Securing quality-of-service route discovery in on-demand routing for ad hoc networks," 2004, 1029120 106-117.

[33] X. Chen and J. Wu, "Multicasting techniques in mobile ad-hoc networks," *The Handbook of Ad-hoc Wireless Networks*, pp. 25–40, 2003.

[34] T. P. Singh, Neha, and V. Das, "Multicast routing protocols in manets," *International Journal of Advanced Research in Computer Science and Software Engineering (IJAARCSSE)*, vol. 2, no. 1, pp. 1–6, 2012.

[35] J. Luo, D. Ye, L. Xue, and M. Fan, "A survey of multicast routing protocols for mobile ad-hoc networks," *Communications Surveys & Tutorials, IEEE*, vol. 11, no. 1, pp. 78–91, 2009.

[36] N. Meghanathan, "Survey of topology-based multicast routing protocols for mobile ad hoc networks," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 3, no. 2, pp. 124–137, 2011.

[37] L. Junhai, X. Liu, and Y. Danxia, "Research on multicast routing protocols for mobile ad-hoc networks," *Computer Networks*, vol. 52, no. 5, pp. 988–997, 2008.

[38] C. Siva, R. Murthy, and B. S. Manoj, *Ad Hoc Wireless Networks Architectures and Protocols*. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2004.

[39] C. K. Toh, *Ad Hoc Wireless Networks: Protocols and Systems*. 1st ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[40] A. C. F. Chan, "Distributed symmetric key management for mobile ad hoc networks," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 4, 2004, pp. 2414–2424 vol.4.

[41] B. Aziz, E. Nourdine, and E. K. Mohamed, "A recent survey on key management schemes in manet," in *Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on*, 2008, pp. 1–6.

[42] R. Anderson, C. Haowen, and A. Perrig, "Key infection: smart trust for smart dust," in *Network Protocols, 2004. ICNP 2004. Proceedings of the 12th IEEE International Conference on*, 2004, pp. 206–215.

[43] V. Gerardo del, G. Roberto, C. mez, and rdenas, "Overview the key management in ad hoc networks," 2005, 2153214 397-406.

[44] W. Bing, W. Jie, B. F. Eduardo, I. Mohammad, and M. Spyros, "Secure and efficient key management in mobile ad hoc networks," *J. Netw. Comput. Appl.*, vol. 30, no. 3, pp. 937–954, 2007, 1231774.

[45] AnilKapil and SanjeevRana, "Identity-based key management in manets using public key cryptography," *International journal of Security (IJS)*, vol. 3, no. 1, pp. 1–26, 2009.

[46] Y. D. Bing Wu, Jie Wu, "An efficient group key management scheme for mobile ad hoc networks," *International Journal of Security and Networks (IJSN)*, vol. 4, no. 2, pp. 125–134, 2009.

[47] D. B. Shacham, X. Boyen, and Hovav, "Short group signatures," in *In Advances in CryptologyCrypto04, Lecture Notes in Computer Science, vol. 3152*, vol. 3152, 2004, pp. 41–55.

[48] R. PushpaLakshmi and A. V. A. Kumar, "Cluster based composite key management in mobile ad hoc networks," *International Journal of Computer Applications*, vol. 4, no. 7, pp. 30–35, 2010.

[49] X. Hai-tao, "A cluster-based key management scheme for manet," in *Intelligent Systems and Applications (ISA), 2011 3rd International Workshop on*, May 2011, pp. 1–4.

[50] ThairKhdour and A. Aref, "A hybrid schema zone-based key management for manets," *Journal of Theoritical and Applied Information Tecnology (JATIT)*, vol. 35, no. 2, pp. 175–183, 2012.

[51] C.-c. Chiang, H.-K. Wu, W. Liu, and M. Gerla, "Routing in clustered multihop, mobile wireless networks with fading channel," in *in Proceedings of IEEE SICON*, 1997, pp. 197–211.

[52] D. Gavalas, G. Pantziou, C. Konstantopoulos, and B. Mamalis, "Clustering of mobile ad hoc networks: An adaptive broadcast period approach," in *Communications, 2006. ICC '06. IEEE International Conference on*, vol. 9, June 2006, pp. 4034–4039.

[53] R. Selvam and V. Palanisamy, "An optimized cluster based approach for multi-source multicast routing protocol in mobile ad hoc networks with differential evolution," in *Pattern Recognition, Informatics and Medical Engineering (PRIME), 2012 International Conference on*, March 2012, pp. 115–120.

[54] C. Bemmoussat, F. Didi, and M. Feham, "Cluster based routing protocol in wireless mesh network," in *Computer Applications Technology (ICCAT), 2013 International Conference on*, Jan 2013, pp. 1–6.

[55] A. EL-SAYED, "Clustering based group key management for manet," in *International Conference on Advances in Security of Information and Communication Networks (SecNet'2013), 3-5 September, 2013, Cairo, Egypt.*, vol. 382, 2013, pp. 11–26.

[56] W. Wei and A. Zakhor, "Multiple tree video multicast over wireless ad hoc networks," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 17, no. 1, pp. 2–15, 2007.

[57] B. R. Tamma, A. Badam, C. Siva Ram Murthy, and R. R. Rao, "K-tree: A multiple tree video multicast protocol for ad hoc wireless networks," *Computer Networks*, vol. 54, no. 11, pp. 1864–1884, 2010.

[58] H. M. Asif, T. R. Sheltami, and E. E. Shakshuki, "Power consumption optimization and delay minimization in manet," in *Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia*, ser. MoMM '08. New York, NY, USA: ACM, 2008, pp. 67–73. [Online]. Available: http://doi.acm.org/10.1145/1497185.1497202

Ayman EL-SAYED received the BSc degree in computer science and engineering in 1994, the masters degree in computer networks in 2000 from the University of Menoufiya, Egypt, and the PhD degree in computer network in 2004 from Institute National De Polytechnique De Grenoble INPG, France. He is an associate professor in the Computer Science and Engineering Department, Faculty of Electronic Engineering, Menoufiya University, Egypt. He is specialized in soft computing, algorithms, and data structure. Also, his interests include multicast routing protocols, application-level multicast techniques, multicast on both mobile network and mobile IP, and image processing techniques. Also, there are other interesting topics such as bioinformatics, biocomputing, and bio computer. He is an approved supervisor for MSc and PhD programs in various University. He has completed various project in government and private organization. He has published more than 45 research papers in international Journals and two books about OSPF protocol and multicast protocols. Currently, he is serving as an editorial board member in various international Journals and conferences. He is a senior member of the IEEE.