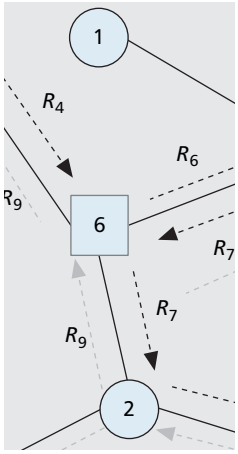
CONSTRUCTING SECURE GROUP COMMUNICATION OVER WIRELESS AD HOC NETWORKS BASED ON A VIRTUAL SUBNET MODEL

YUEH-MIN HUANG, CHING-HUNG YEH, AND TZONE-I WANG, CHENG KUNG UNIVERSITY
HAN-CHIEH CHAO, NATIONAL ILAN UNIVERSITY



The authors propose a virtual subnet model to construct a secure group communication over a MANET. With the model, the composition of groups is established as the forming of group keys.

ABSTRACT

Recently, more and more people have begun using mobile devices such as PDAs and notebooks. Our lives have been profoundly affected by such devices. A MANET, a mobile ad hoc network, is an effective networking system facilitating an exchange data between mobile devices, without the support of wireless access points and base stations. A MANET is not restricted to unicast or multicast communication, but can also provide "many-to-many" transmission, which can be treated as a group communication. Until recently, however, the way in which such groups are formed had not drawn much attention. Because communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive information being intercepted by unintended recipients is a real concern. Consequently, efforts to ensure the security of group communications in MANETs are essential. This article proposes a virtual subnet model to construct secure group communication over a MANET. With the model, the composition of groups is established as the forming of group keys. Our results show that this approach can completely satisfy the needs for both security and efficiency.

INTRODUCTION

With the progress in networking technology, there has been a tremendous amount of data exchange and sharing. Virtual local area network (VLAN) is one effective technology to enable computers on different networks to communicate simply and efficiently [1]. A VLAN operates like a general LAN, but also works if the devices do not have a physical connection in the same network segment. When devices need cross-regional communication, they can be located anywhere on a wide area network; VLAN technology can group them together, and information can be exchanged as simply as in a LAN. In wireless communication, a mobile ad hoc network (MANET) [2] is a system made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics; hence, they can freely form communication groups as necessary. In general, a particular application or interest in a network may lead to the establishment of a corresponding community. It seems to be inevitable that more than one communication group may exist in the same MANET. Thus, it is necessary to partition the network into multiple domains by communication groups as in a VLAN. Meanwhile, this also implies that many groups propagate packets simultaneously. However, through transmission in a broadcast manner these data packets can be received by all groups or nodes, including those that do not need or should not receive them. As a result, sensitive information is exposed publicly in an unprotected situation. Although many studies have resolved security issues in wireless networks, such as mesh networks [3], sensor networks [4, 5] and intercluster key management [6], to the best of our knowledge group construction and secure group communication have not drawn much attention.

In this article we design a virtual subnet model in a MANET to construct group communication, and propose applicable mechanisms to achieve security and improve communication efficiency. There is an initiation stage to assign related parameters, a creation stage to construct groups, and a group key agreement stage to share the secure key in a group. In addition, we provide the maintenance and transmission mechanisms that cooperate to achieve the virtual subnet behavior and communication.

The remainder of this article is organized as follows. First, we describe VLAN and group key distribution, and then discuss the construction of groups in a MANET, including the initiation stage, creation stage, and maintenance and transmission mechanisms. After that, the detailed group key agreement in our virtual subnet model is presented. Finally, we make con-

1536-1284/07/$20.00 © 2007 IEEE

cluding remarks and identify some possible directions for future study.

Related Work

Virtual Local Area Network

In the traditional switched LAN, broadcast and multicast packets are always forwarded to all devices, even to nodes that do not require them. The IEEE 802.1Q [7] standard was developed to solve the problem of how to segment a large network into smaller ones so that broadcast and multicast traffic do not snatch more bandwidth than necessary. The mechanisms in IEEE 802.1Q are a logical collection of network devices, and include how the frames are relayed to destinations and frame format. The major points are:

- Any frame belonging to a VLAN has a VLAN-tag to associate with the VLAN ID (VID).
- The filtering database (FDB) stores the addressing information of all groups (nodes), even if they are unrelated.

VLAN-aware switches can provide the intelligence to make filtering or forwarding decisions for packets, and then communicate with other switches and routers within the network.

First of all, when a frame arrives at the VLAN-aware switch, it is checked for errors. Obviously, error frames are dropped, and error-free frames are associated with a VID. If the ingress filter (source port filter) is set to enable and the incoming port is not a member of the same VLAN, the frame is rejected.

Second, the accepted frame enters the forwarding process to be relayed to other ports; meanwhile, the switch studies the frame's information, such as associated VID and necessary data, and then automatically uses it to update the FDB if required. The forwarding process uses the MAC address and VID of the frame indices to the FDB to search for where the frame needs to be relayed.

Finally, the frame is sent to its corresponding outbound port if it is not filtered out by the egress filter, which diagnoses whether or not the outgoing frame is carrying a correct VID.

The VLAN exploits the VID, filter, and FDB to segment networks, providing the key points to construct virtual subnets in a MANET.

Group Key Distribution Protocol

Key exchange is the foundation of secure group communication. In the original literature, the two-party Diffie-Hellman key exchange protocol was proposed in 1976 [8]. There are two well-known system parameters in the protocol: q is a prime number, and a is an integer that is less than q. If A and B need to share a secure key, they create random private values X_A and X_B, respectively. Then they generate their public values by the parameters q and a. A's public value is $Y_A = a^{X_A} \bmod q$ and B's public value is $Y_B =$ axb mod q. Finally, they exchange their public values; A and B share a common secret key by the following equation:

$$(Y_B)^{X_A} \bmod q = (a^{X_B} \bmod q)^{X_A} \bmod q = (a^{X_B})^{X_A} \bmod q$$

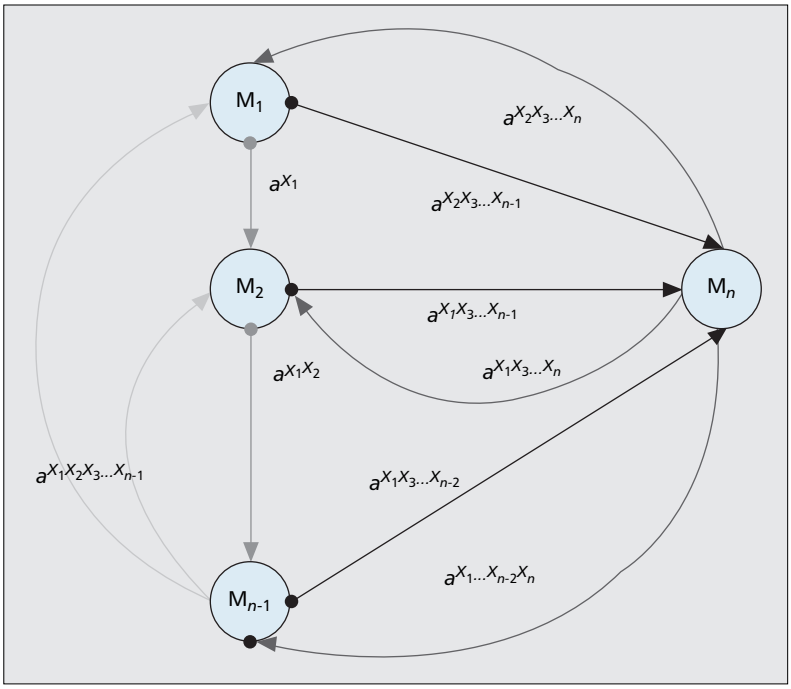


Figure 1. *Group Diffie_Hellman.3 procedure.*

$$= (a^{X_A})^{X_B} \bmod q = (a^{X_A} \bmod q)^{X_B} \bmod q = (Y_A)^{X_A} \bmod q$$

In 1996 [9], the Diffie-Hellman key exchange protocol has extended to n-party setting, and the security is as robust as the original two-party protocol.

The GDH.3 in [9] comprises four steps, assuming all participants $M_1, \ldots, M_n$ agree to share a secure key. In the first step each individual, M_i, provides its contribution Y_i to M_{i+1} by upflow, where $1 \leqq i \leqq n - 2$. Next, M_{n-1} processes the final upflow message to obtain $a^{X_1X_2X_3\ldots X_{n-1}}$ and broadcasts this value to all other participants. In the third step, participant M_i $(i \neq n)$ receives the value $a^{X_1X_2X_3\ldots X_{n-1}}$, factors out its own exponent, then forwards the result to M_n. In the last step, M_n receives each value from the previous stage, raises its power X_n to every one of them, and broadcasts the resulting n –1 value to the rest of the group. At this stage, each M_i has a value with the form $a^{\Pi\{X_j | j \subset [1..n] \wedge j \neq 1\}}$ and can compute the common group key. Figure 1 shows the GDH.3 procedure.

Based on the description above, the group members know each other. However, it is difficult for a node to know other members of the group in advance in a dynamic MANET, which results in a chaotic situation while endeavoring to establish the security of group communications. Our model is designed to solve this situation with both group construction and group key exchange for secure communication.

Constructing Groups in MANETs

With intelligent mobile devices likely to be even more popular in the future, MANETs will be extensively used in many circumstances and envi-

Neighbor status / Group	Existing neighbor	Nonexisting neighbor
Same	Reply VS-REPLY packet and relay VS-REQUEST packet	Reply VS-REPLY packet and discard VS-REQUEST packet
Different	Relay VS-REQUEST packet	Discard VS-REQUEST packet

Table 1. *The nodes' behavior on receiving the VS-REQUEST packet.*

ronments, such as conferences, playgrounds, parks, and other large places accommodating many people. In such locations there are many groups that need to communicate by intelligent mobile devices. However, the mobile multihop property of MANETs is insufficient for efficient and secure group communication; therefore, it must construct virtual subnets. Groups are formed because of a common interest or topic, but the question arises as to how they distinguish the common topic in wireless broadcasting. In this model we design an agent node that takes charge of announcing public and predefined topics or accepting and registering new topics, and assigning to them the necessary corresponding parameters. The agent node can be the chairperson of a conference, the manager of a park, or a person in any other comparable role; and this role can have temporary or long-term responsibility. We also design three rules to serve the virtual subnet in a MANET:

- Each packet includes a virtual subnet identification (VSID) field in the packet header to identify to which virtual subnet it belongs. If the field is null, the packet is a general (non-virtual-subnet) packet.
- Each node creates a forwarding cache table to store the VSID as a filter that can detect whether the packet is relayed or not.
- Each node inserts a VSID into the forwarding cache table after receiving a cache request (CREQ) packet contained in hello messages to advertise that the virtual subnet exists.

According to the above premises, groups can be constructed on a virtual subnet model by the initiation, creation, and group key agreement stages to let nodes cooperatively generate the group key. Furthermore, the maintenance and transmission mechanisms are coupled to achieve the virtual subnet behavior and packet propagation, and they are enabled immediately when the virtual subnet is composed in the creation stage. These components are described below.

Initiation Stage

When a node arrives at a specific area of the ad hoc network, it goes to the agent node to register its topic of interest, or it can create a new topic in the agent node while waiting to register. Meanwhile, the agent node prepares an individual hash function $h()$, and security parameters q and a for each group. While a node registers a group or creates a new group, the agent node assigns the corresponding $h()$, q and a to the node. Since the agent node is in charge of the specific area, it is reasonable to assume that the agent node will act in a secure region free of counterfeit agent nodes, and as a result, the registering and assigning procedures are fully safe.

For the confidentiality of the groups, the agent node neither directly assigns the VSID nor involves the group key generation in the creating procedures, but lets them be generated by all the participants.

Creation Stage

The network consists of N nodes, and they are randomly distributed over a specified region after they contact the agent node. We consider in the source-initiate communication that the communication request and session duration can be randomly generated at each node that is permitted to initiate a virtual subnet.

When a source node needs to communicate with a group that is registered but still has no VSID, the source node broadcasts a VS-REQUEST packet including $<Nonce_s, ID_s, h(Nonce_s||ID_s)>$ as an advertisement. Other nodes receive this VS-REQUEST packet and can identify whether the source node is in the same group or not by inspecting h(Nonces|| IDs). When a node receives $<Nonce_s', ID_s', h(Nonces||ID_s)>$, the node can compute $h'(Nonce_s'||ID_s')$ to compare whether $h(Nonce_s||ID_s) = h'(Nonce_s'||ID_s')$. Because the same group has the same $h()$, this inspection can easily be verified, and the reaction of receiving VS-REQUEST nodes is to reply with a VS-REPLY packet, including $<Nonce_i, ID_i, h(Nonce_i||ID_i)>$ or discard the VS-REQUEST packet. The relaying VS-REQUEST packet is also an obligation that is influenced by the neighbors' relation of receiving VS-REQUEST nodes. This decision is presented clearly and simply in Table 1.

The source node collects the IDs of group members from receiving VS-REPLY packets and inserts them into the virtual subnet member list in ascending order. Similarly, the source node inspects $h(Nonce_i||ID_i)$ via $h()$ to identify whether the replying node is in the same group or not. After a period of time, other nodes will receive the VS-REQUEST packet, and the same group nodes reply to the source node with a VS-REPLY packet. The source node then adopts its own ID to be the VSID and propagates the virtual subnet information $<$ *Nonce*$_s$, *ID*$_s$, *VSID*, *virtual subnet member list*, $h(Nonce_s||ID_s)>$ to the same virtual subnet member by multicasting. Note that $h()$ is an identified and inspected utility, so nodes in the same virtual subnet know each other, and VSID can be included in each packet for group communication.

In the example of network topology shown in Fig. 2, there are a triangle, a circle, and a square representing three virtual subnets. We demonstrate the square virtual subnet, which consists of nodes 4, 6, 7, 9, and 12.

Assume that node 6 is the source node, and it needs to communicate with the virtual subnet, but the VSID is null. Node 6 broadcasts a VS-REQUEST including $<Nonce_6, ID_6, h(Nonce_6||ID_6)>$. Other nodes will receive the VS-REQUEST packet from node6. If any node receives duplicate VS-REQUEST packets from the same source node, it only processes the first one received and drops the other one. According to Table 1, each node performs the corresponding action.

For nodes 3, 10, 2, 8, and 11, their $h()$ are