Research on the Implementation of VoIP Service in Mobile Ad-hoc Network

[1,2]Yi Sun, [1,2]Gengfa Fang, [1]Jinglin Shi

([1]Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, P.R. China;
[2]Graduation School of the Chinese Academy of Sciences)

{sunyi@ict.ac.cn, gengfa.fang@ict.ac.cn, sjl@ict.ac.cn}

Abstract

Traditional way to implement VoIP application on hard-wired network is based on the fixed and invariable IP addresses of the source and destination nodes. However, in Mobile Ad-hoc Network (MANET), the IP address of each node is auto-configured and may change at any time. Therefore, the traditional way cannot be applied on MANET. This paper presents a new way to design VoIP application on Mobile Ad-hoc Network, which can correctly solve the problem of variable IP addresses in MANET and make the nodes communicate with each other reliably.

1. Introduction

1.1 The Necessity of Implementing VoIP in MANET

The VoIP (Voice over IP) technology has been a hot issue for the last ten years in IT industry [1].

MANET (Mobile Ad-hoc Network) [2] is a kind of self-organizing networks. In it, mobile nodes could communicate with one another without any communication infrastructure such as base station or access point.

Nowadays people often use interphones as communication tools in a LAN (local area network) scope. But interphone has its inherent disadvantage: the frequency band is open to everyone and shared with different users. So if there are more than one communication groups existing, they might interfere with each other by using the same frequency occasionally or purposely—people would hear other person's talk.

VoIP technology is converting voice signals to data packages and transferring them on IP network. Every package definitely has its destination address, so other nodes cannot receive this packet. By this way different communication groups can avoid interfering with each other. What's more, we can make use of the network security procedures such as encryption to improve the safety of communication further. So it is desirable and necessary to implement VoIP in portable MANET equipments (PDA, Notebook PC etc.) and use these equipments as communication tools in LAN.

1.2 The Challenge of Implementing VoIP in MANET

Unfortunately, traditional way to implement VoIP in fixed network does not work in MANET. In MANET, to alleviate user's burden, the IP addresses of the nodes may use auto-configuration process [3]. And the auto-configured address must be proven to be unique in MANET through DAD (Duplicate Address Detect) [4] [5] test before the node uses it.

However, even though the address of the node passed DAD test successfully, it still cannot be assured that the node would use this address in its whole lifetime. Under some conditions, the node has to change its address.

Condition1:
Node A moved outside the MANET and at the same time Node B entered the MANET. It happened that Node B chose the same address as Node A and passed DAD test successfully, because Node A lost connection at that time. So Node B announced it has the same address as Node A. But after a while, Node A moved back and resumed connections with other nodes. Now Node A and Node B have address conflict, and one of them will have to change its address.
Condition2:
Two separate MANETs moved towards and merged into one MANET finally. Because the two MANETs are independent to each other originally, there may be some duplicate addresses between them. Thus when they merged into one, address conflicts occurred. As the result, some nodes need to change their addresses.

Traditional way to implement VoIP is based on the fixed IP addresses of the nodes, taking no consideration of the address variety in MANET. In this paper, we raise a scheme to implement VoIP in MANET, and ensure users to convey voice reliably. This paper is organized as follows: Section 2 presents our scheme in details. Section 3 explains how our scheme solves the variable address problem in MANET. Section 4 briefly describes our implementation and introduces our future work.

2. Our Scheme

2.1 Premises

The implementation of our scheme is based on two premises.

First, because the IP addresses of the nodes in MANET are variable, we cannot initiate a phone call through IP address. Instead, we designate a Communication ID for each node, and use this ID to make a phone call. Communication ID must be absolutely unique (this means it is unique in the world) and invariable. It can identify a node and should be easily remembered by users. To guarantee the uniqueness of Communication IDs, we propose a special organization to distribute and maintenance these IDs.

Second, we import authentication process into our VoIP scheme to enhance the reliability of the phone call. To do so, we request every node has a public key and a private key. The nodes must know each other's public key before they make a phone call.

As for how to get the genuine public key of nodes in MANET, we could adopt key pre-sharing method or we could make use of a similar scheme introduced in reference [6]. But in reference [6], it does not consider the variability of IP address in MANET, so public key is bound with IP address. And in our implementation, the public key is bound with the unique and invariable Communication ID of the node.

2.2 The Setup Process of a Phone Call

When a node wants to initiate a call to another node, it should produce a random number in the first place. Then the caller node should encrypt the random number with the public key of the callee node and the private key of itself. The random number will be used later in the authentication process. Next, the caller node visits Name Service Module in it, and try to get the IP address of the callee node. Name Service Module is fit for maintaining a local database. The database includes a series of records, each of which contains the Communication ID and IP address of one node. These records are reserved from call history. However, the call history may not tell the current IP address of the callee node, because the callee node would change its IP address after the previous phone call. So we cannot use the IP address that the Name Service Module returns to

set up the voice link. Instead, we send a single-cast inquiry message to verify the IP address the Name Service Module returns. The format of the single-cast inquiry message is shown in Fig.1. If the local database does not contain the corresponding record, Name Service Module would return Null. Then we would have to send multicast inquiry message to get the current IP address of the callee node.

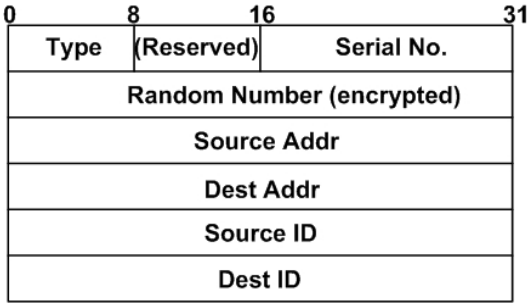

Fig.1 **Format of single-cast inquiry message**

"Type" field indicates the type of the message, and for single-cast inquiry message the value of this field is 0. "Serial No." points out the serial number of this inquiry. The node would have sent a lot of other inquiries, so we need a field to signal the inquiry for this time. And the node increases the value by 1 every time after it sends a new inquiry. "Random Number" contains the random number that caller node produces for the voice communication and it is encrypted. "Source Addr" and "Dest Addr" present the source and destination address of the inquiry message. "Source ID" and "Dest ID" indicate the Communication ID of caller and callee node.

When the single-cast inquiry message reaches the destination node, that node checks the value of "Dest ID" field in the inquiry message and compares it with the Communication ID of itself. Then the node sends a reply message to the caller. The format of reply message is shown in Fig.2.

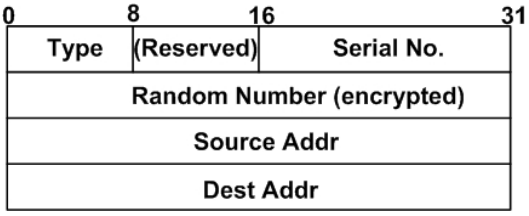

Fig.2 **Format of reply message**

"Type" field indicates the type of the message, and for reply message to single-cast inquiry the value of this field is 1. "Serial No." points out the serial number of the inquiry to which it replies, and the value is copied from the same field of corresponding inquiry message. "Source Addr" and "Dest Addr" present the source and destination address of the reply message. If the Communication ID of the node match the "Dest ID" in the inquiry message (it means it is the callee node), the node would decrypt the encrypted "Random Number" in the inquiry message with the private key of itself and the public key of the caller node (the caller node is indicated in the "Source ID" field of the inquiry message). The callee node then stores the decrypted random number for use of authentication process later. Next, the callee node would encrypt the random number with the public key of the caller and the private key of itself, and write the result into the "Random Number" field of the reply message. If the Communication ID of the node and the "Dest ID" field of the inquiry message don't match, we simply use "0" to fill the "Random Number" field of the reply message.

If caller node receives reply message within a given time, it decrypt the "Random Number" of the reply message with the private key of itself and the public key of callee node. Then caller node compares the result with the original random number it chose for the call. If the two numbers are identical, it means authentication process of the callee node passes. Then we can use the IP address the Name Service Module returned to set up the voice link. Otherwise, if caller node doesn't receive reply message in

time or the two numbers are different, it means the IP address that Name Service Module returned is invalidated. Then caller node must send multicast inquiry message to get the current IP address of the callee.

The format of the multicast inquiry message is the same with that of single-cast inquiry message. See Fig.1. The "Dest Addr" field in the multicast inquiry message is filled with multicast address and the message would be sent to every node in MANET. The value of "Type" field is 2 for multicast inquiry message.

Every node in MANET receives multicast inquiry message and check if it matches the "Dest ID" for the voice call. If it does, the node is the callee node of the voice communication and it must send a reply message, telling its current IP address to the caller. The format of reply message is shown in Fig.2. The value of "Type" field is 3 for reply message to multicast inquiry.

If caller node receives reply message within a given time, it decrypt the "Random Number" of the reply message with the private key of itself and the public key of callee node. Then caller node compares the result with the original random number it chose for the call. If the two numbers are identical, it proves the message is indeed sent by the callee, because only callee node could correctly decrypt the encrypted "Random Number" in the inquiry message. So caller node get the current IP address of the callee from the "Source Addr" field of reply message and it first updates local database then set up voice link using this address. If the two numbers are different, the caller would discard this reply message. If caller doesn't receive correct reply within a given time after it sends multicast inquiry message, it means that the callee node is unreachable at this time and the voice call ends with an error.

2.3 Voice Link Maintenance in the Call

When the two sides get each other's IP address, they could establish voice link and enter the calling state. During the communication time, the endpoints may still have to change their IP address for some reason. So we should design a method to ensure that the voice link would not be falsely hold due to the IP address changes of the endpoints.

To achieve above object, we require the two endpoints of the call send control messages periodically to tell its current IP address to each other. Format of the address noticing message is shown in Fig.3.

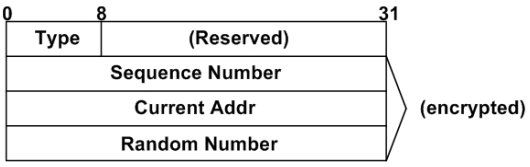

Fig.3 **Format of address noticing message**

"Type" field indicates the type of the message, and for address noticing message the value of this field is 4. 32 bits "Sequence Number" is used to resist replay-attack and out-of-order arrival. "Current Addr" points out the current IP address of the node. "Random Number" includes the random number the two endpoints negotiated during the set-up state of the voice link and it is used for authenticating. The last three fields is encrypted before address noticing message is sent.

When one side of the call receives address noticing message from the other side, it first decrypt the message and check if the "Random Number" in the message is the same with the number negotiated at the handshake. If it is not, simply discard the message. Otherwise (indicating the message is from the other party of the call, because only the two endpoints of the call know this random number), check the "Sequence Number" in the message to see if the message is new. If the message is old, discard it. Or else, compare the "Current Addr" in the message with the IP address of the other party being used. If they are different, it means the other party of the call has changed its IP address.

So the node would redirect the voice link to the new IP address.

We stipulate the two endpoints of the call send address noticing message periodically, and increase their respective sequence number by 1 every time they send a new message. If the endpoint doesn't receive any correct new address noticing message from the other party within a given time, it would release the current voice link.

3. Analysis and Estimates

So far, we have introduced our scheme to reliably implement VoIP in MANET environment. Next, we simply estimate our scheme.

3.1 Voice Link Setup

Before the voice link establishes, the two parties shares a random number through a handshake process. Because the random number is sent all in cryptograph, other nodes in MANET cannot know it. Thus, the random number could act the evidence in authentication. Besides, we don't use the IP address that the Name Service Module returns to set up voice link directly. Instead, we send a single-cast inquiry message to test the validity of the address before we use it to build the connection. By doing this, we enhance the reliability of the voice call in MANET environment. Sending single-cast inquiry message other than sending multicast inquiry message every time to get the address, could alleviate the problem of broadcast storm which is a very important issue in MANET.

3.2 IP Address Changes During the Call

In our scheme, each endpoint of the call would periodically send address noticing message to tell its current IP address to the other. Therefore, if one side changes it address, it would tell its new address to the other side in time through address noticing message. The other side decrypts the message and switches the voice link to the new address. Because address noticing message contains the random number which is only known by the two parties of the call, we could judge whether the message is indeed from the other party. Adding "Sequence Number" field into the message could resist the replay-attack as well as out-of-order arrival problem.

If the two endpoints of the call change their IP addresses for one or more times in turn, according to the analysis above, the voice link could still be correctly hold.

But if the two endpoints of the call change their IP addresses at the same time, both of the address noticing messages they send cannot reach the destination. So the two parties have no idea of the fact that the other side has already changed its address. Under this condition, the link cannot be rightly held, but at least we need a method to notice the node of the error information so that the node would release the link in time. As we illustrated in 2.3, when one endpoint hasn't received any new correct address noticing message for a given time, it would release the current voice link. By this mechanism, even though the IP addresses of the two endpoints change simultaneously, after a while the link would also be released due to absence of new correct address noticing message. Therefore, the voice link couldn't be wrongly held for a long time.

3.3 The Limitation of the Scheme

Our scheme could ensure the reliable voice communication in MANET, but it still has some limitations.

Firstly, to enhance reliability we add a handshake before the voice communication process, thus added the set-up time slightly.

Secondly, we stipulate the endpoints periodically send address noticing messages, increasing the load of the network.

Lastly, we need to point out that our objective is to resist the bad effect of variable IP address in MANET on VoIP application. At the same time, because we adopting some network security procedures such as authentication and encryption, our scheme also enhance the security of the voice communication to a certain extent. However, our scheme doesn't aim at improving security. The common security problems in MANET like eavesdropping, counterfeiting and evilly forwarding are not within the scope of this paper.

4. Summary

Our scheme is implemented as follows:

At the handshake stage, we adopt unsymmetrical encryption algorithm—RSA [7]. In order to reduce the creating time of large prime number, we demand the length of the key is only 8 bits.

If a node doesn't receive correct reply in 2 seconds after sending inquiry message, it would initiate appropriate timeout operations. The value of this time is set according to the size of network, the process ability of node etc. And it could be estimated using the following formula.

WAIT_TIME = 4*NODE_PROCESS_TIME*NET_DIAMETER

Wait_Time: time node need to wait before initiating timeout operations.

NODE_PROCESS_TIME: the process time of the node. It is the sum of processing time and message-forwarding time. The default value is 40ms.

NET_DIAMETER: the maximal hops between two nodes in MANET. It is closely related with the size of network.

During the communication, endpoints send address noticing message to each other every 5 seconds. For the efficiency consideration, we adopt symmetrical encryption algorithm—RC4 [8] to encrypt address noticing message and the key of RC4 is just the random number negotiated in handshake.

At last, we stipulate endpoint would release voice link if it hasn't received any new correct address noticing message for 30 seconds.

To summarize, we raise a scheme to implement reliable VoIP application in MANET. It eliminates the bad effort of the variable IP address in MANET on the voice communication.

So far, our work is aiming at point-to-point single-cast VoIP application in MANET. In future, we would focus our attention on the multicast VoIP application such as meeting system, considering how to solve the more complex problem of address changes in multicast environment.

Acknowledgement

This work was supported by the Digital Olympics in Key Technologies R&D Program (Grant No. 2003BA904B06)

References

[1] http://www.chinaitlab.com/www/spe cial/voip.asp

[2] Ramanathan R, Redi J, "A Brief Overview of mobile Ad-hoc Networks: Challenges and Directions", IEEE Communications Magazine, 50th Anniversary Commemorative Issue[C], pp. 22-25, 2002

[3] K. Weniger and M. Zitterbart, "IPv6 autoconfiguration in large scale mobile ad-hoc networks", In Proceedings of European Wireless 2002, Florence, Italy, February 2002

[4] Nitin H. Vaidya, "Weak Duplicate Address Detection in Mobile Ad-hoc Network", In MOBIHOC'02, June 9-11, 2002, EPFL Lausanne, Switzerland

[5] Kilian Weniger, "Passive Duplicate Address Detection in Mobile Ad-hoc Network", In IEEE WCNC 2003, March 2003

[6] Asad Amir Pirzada, Chris McDonald, “Kerberos Assisted Authentication in Mobile Ad-hoc Network”, In 27th Australasian Computer Science Conference, Dunedin, New Zealand, January 18-22, 2004

[7] B. Kaliski, J. Staddon, “PKCS #1: RSA Cryptography Specifications Version 2.0”, IETF RFC2437, 1998

[8] William Stallings，“Cryptography and Network Security, Principles and Practices (Third Edition) ”, Publishing House of Electronics Industry