Creation and Management Method of a Secure Connection on MANET using Multi-Hop Routing Protocols

Masato OGUCHI and Mio KAMADA

***Abstract*— Mobile Ad hoc Network(MANET) is an autonomous distributed network constructed only with gathering nodes temporarily, which has no connection with existing infrastructures like Internet. In MANET, wide area communication through wireless networks is realized as nodes in the network can relay other node's data packets using a multi-hop routing protocol. In the case of wireless networks, especially in MANET, it is required to secure the data transfer by encryption because communications on wireless networks are easy to be eavesdropped and falsified in contrast to that of wired networks.**

We have proposed a mechanism to create and manage encrypted connections for secure communications in MANET. In this paper, we have established a communication route using OLSR as a multi-hop routing protocol, and introduced methods to control secure connections by applying IPsec as an encryption scheme. In addition, besed on the proposed method, we have implemented the acquisition mechanism of an IP address, created and reconfigured of secure connections in consideration of security problems in MANET.

I. INTRODUCTION

Recently, various kinds of communication networks are realized as communication technologies progress. Among them, Mobile Ad hoc Network (MANET)[1], configured only with terminals that equip a wireless LAN interface and have no connection with existing infrastructures like Internet, is attracting attention. In MANET, when nodes are distributed in a wide area and each node cannot communicate directly with all nodes in the network, some nodes on a route relay the data transfer so that wide area communications can be realized. This is called a multi-hop network, shown in Figure 1. In a multi-hop network, each node works as a router also, based on a routing protocol that takes care of data transfer routes in the network. Thus it is always possible to communicate on a multi-hop network regardless of its change of configuration, as nodes join and leave the network. Multi-hop networks are expected as a basic mechanism of vehicle-to-vehicle communications in ITS, ubiquitous networks, and so on.

Generally, wireless communications tend to be eavesdropped and/or falsified easily. Therefore, security problems in such an environment should be examined. Especially in MANET, since unspecified nodes can participate in the network, that is to say, unknown nodes may exist on a data transfer route, developing more elaborate security methods are inevitable. It is possible to use existing encryption and/or authentication mechanisms for a wireless LAN, which guarantees an equal security level to all nodes in a network. However, in a multi-hop network, existing security mechanisms are not necessarily useful since it is difficult to encrypt only a specific data transfer route between specific nodes. In addtion, even though MANET is always changing its configuration, the existing security mechanisms do not consider about such a feature of MANET.

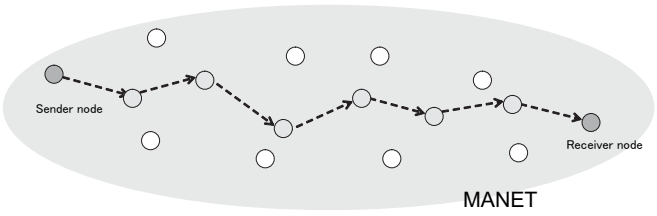

Fig. 1. Multi-hop network

Security mechanisms for MANET are coming to be studied currently. However, most of them assume only an environment in which an access point exists and each node can at least connect an infrastructure network temporarily. In the case of a multi-hop network, secure data transfer with no infrastructure should be required, like vehicle-to-vehicle communications. Therefore, a security method that works even with the change of network configuration must be considered. Although some secure routing methods are also studied[2][3], most of them aim to develop a new routing protocol with embedded encryption mechanism, and evaluate it with a simulation. Several authentication mechanisms suitable for MANET are also studied[4][5].

In this paper, a model that connects and manages an encrypted data transfer route is proposed, thus secure communications become possible on a multi-hop network. Optimized Link State Routing (OLSR), an existing MANET routing protocol, is utilized for creation of a route that constructs a multi-hop network, and data transferred on the route is encrypted for secure communications. Such a route is called a "secure connection" in the rest of this paper.

Researches about securing OLSR are also reported[6]. However, this types of security requires PKI and/or timestamp based authentication, which is not necessarily suitable for MANET. Discussions about implementation and analysis of Intrusion Detection System (IDS) for OLSR are also published[7]. Our idea simply uses public key of each node for the authentication and encryption. This is more suitable

M. Oguchi is with Department of Information Sciences, Ochanomizu University, 2-1-1, Otsuka, Bunkyo-ku, Tokyo, Japan. oguchi@computer.org

M. Kamada is with Department of Information Sciences, Ochanomizu University. Currently with Nissan Motor Co., Ltd.

for Peer-to-Peer communication in MANET, since it may be difficult to connect backbone infrastructure like Internet. Securing only communication with partners, whose public keys are held mutually, may be desired in such a case. Moreover, our idea is more realistic solution for security of MANET, since widely-used existing security mechanisms such as IPsec can be employed.

II. Background of our research work

A. Security techniques for wireless LAN

Communication protocols in a network have hierarchical structure generally. In the case of encrypted communications also, several methods for encryption exist at each layer, used for various objectives of communications. At present, Wireless Equivalent Privacy (WEP), encrypting data in the Data Link Layer, is a basic standard in wireless communications. However, WEP seems to include several problems. For example, a secret key should be shared among all terminals in a network, the length of the key is said to be too short, and the way to apply the encryption algorithm, RC4 in WEP, is pointed out not to be secure in some cases.

Afterwards, an encryption protocol that reinforces WEP, called Temporal Key Integrity Protocol (TKIP), is proposed. A security standard called Wi-Fi Protected Access (WPA), which supports TKIP and authentication framework IEEE802.1X, is also formed. Moreover, IEEE802.11i, which is a superset of WPA, is ratified finally. This supports strong encryption algorithm, Advanced Encryption Standard (AES), and has a function to renew and exchange a secret key after authentication. Generally in these security specifications, authentication servers are assumed to be located on a fixed infrastructure connecting through an access point.

B. Security problems in a multi-hop environment

When these existing security techniques are applied, the following problems will occur in a multi-hop network. First, the current security standard, WEP, assumes a secret key is shared among all nodes on the spot. In such a case, it is possible to provide the same security level to all nodes existing there. However, it is difficult to apply WEP when a specific connection, one of multi-hop connections in MANET, is needed to be protected. Above all, WEP is not considered to be secure enough anymore.

As mentioned above, the advanced security technologies including WPA and IEEE802.11i can be used in the latest wireless LAN. These specifications can be applied to networks that include a fixed infrastructure on which servers are located. However, it is difficult to apply them to a multi-hop connection in MANET.

Thus another way of encryption must be considered when temporal and autonomous communications like MANET are realized. In this paper, such a mechanism works on a multi-hop network is proposed and implemented. IPsec is employed for the ease of its implementation, which encrypts transferred data in Network Layer.

C. Multi-hop routing protocol

In a multi-hop network, communications between nodes that cannot talk directly with each other are relayed by other nodes in MANET. In order to realize such a mechanism, a multi-hop routing protocol is used for finding a route between a sender and a receiver. In MANET, a communication environment is always changing. That is to say, any node may move, join, and leave the network at anytime. In addition, low bit rate and volatile wireless connections are used generally. A lot of protocols, taking these matters into account, are proposed until now.

Routing protocols in MANET are classified into two types; proactive and reactive. In the proactive type, nodes in the network constantly exchange routing information, so that they always know the route to other nodes in MANET. Each node in the network keeps next hop information on its routing table; therefore a route is created instantly upon a request. However, because the routing information is always exchanged, such communications might be in no use depending on the change of the network configuration. Examples of proactive type routing protocols include Optimized Link State Routing (OLSR)[8] and Topology Broadcast based on Reverse-Path Forwarding (TBRPF)[9].

In reactive routing protocols, on the other hand, a route from a sender to a receiver is searched upon each communication request. This causes a delay as a packet is sent only after the route to the destination is searched, found, and established. Some of well-known reactive type routing protocols are Ad-hoc On-demand Distance Vector (AODV)[10] and Dynamic Source Routing (DSR)[11].

In this paper, since it is better the route has been already established when a secure connection is required, OLSR, one of the most famous proactive routing protocols, is employed.

III. Method of constructing a secure connection

A. An overview of a secure connection

MANET is not always a secure environment because it is a public network generally. That is to say, unspecified nodes can join and they might relay communications in a multi-hop network. Thus a secure connection, which encrypts communications between a sender and a receiver in MANET, is desired as shown in Figure 2. This connection is needed when two nodes, trusted with each other, communicate through a multi-hop network.

In this research work, secure connections are created by encrypting transferred data with IPsec. Therefore, the method of establishing IPsec Security Association (SA) in MANET is discussed, leaving the routing protocol itself to OLSR. Since a node in MANET usually does not have a fixed address, a method to resolve the address must be considered when IPsec, designed basically for a wired communication, is applied.

Thus in this paper, considering the encryption key and other problems, a mechanism to create and manage a secure connection in a multi-hop network is proposed, in which routing is executed by one of MANET protocols – OLSR

for example. In this proposed method, a trusted nodes list is created and managed, which is used when a secure connection is established. After the node joins MANET, the destination node's ID is corresponded with IP address used in the network, and the information is registered on the trusted nodes list. As a result, a secure connection with a trusted node can be created based on the information. The details of the proposed method are described in the following subsections.

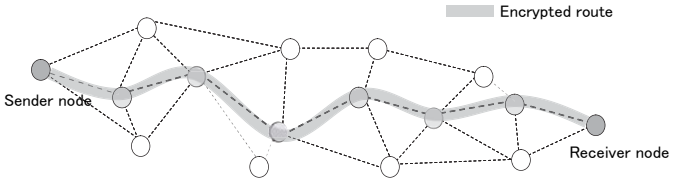

Fig. 2. Secure connection

B. Management of trusted nodes list

1) Creating ID and public key list: In multi-hop communications, encryption is required only when the both end nodes are trusted with each other. Therefore in this proposal, each node holds a trusted nodes list in advance, and information required for establishing a secure connection is also stored and managed in the list. Because each node generally does not have a fixed address in MANET, they are distinguished using IDs. When a secure connection is created, a public key held by each node can be used. Thus, each node stores pairs of ID and a public key of trusted nodes in advance, and adds IP address information of this node after it joins to MANET. This public key is used only when a connection is established in Internet Key Exchange (IKE) phase, a connection establish phase in IPsec, not used in encryption itself in IPsec.

When an encrypted communication is required with members in the list, this information is used and a secure connection is established. As a result, even if an eavesdropper or other malicious nodes exist on a route of data transfer, secure communications become possible. By keeping information only about trusted nodes in the list, it is possible to distinguish the right counterpart of communication even in a multi-hop environment in which direct communication is impossible.

2) Updating the list: A secure connection is created only with a trusted node. When a trusted nodes list is created, a security-guaranteed trusted group is configured, and members of the group exchange information about trusted nodes. Only authenticated nodes can join the group, and they exchange information of trusted nodes' IDs and public keys, and add them to the list as shown in Figure 3. When a node needs to communicate with a group member, nodes on the list are guaranteed to be secure, thus it is possible to create a security connection immediately using the information on the list.

On the other hand, if an encryption communication is required with a node which is not on the trusted nodes

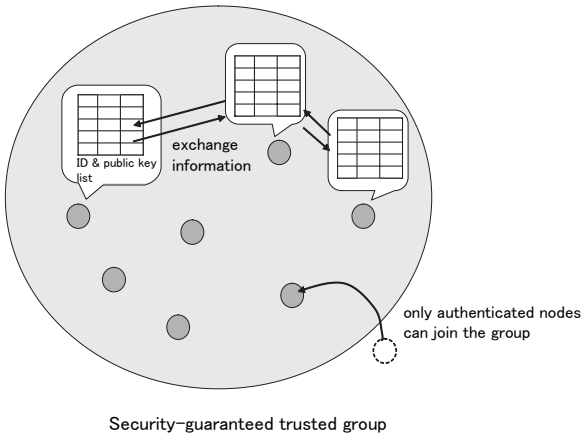

Fig. 3. Creating and updating a trusted nodes list

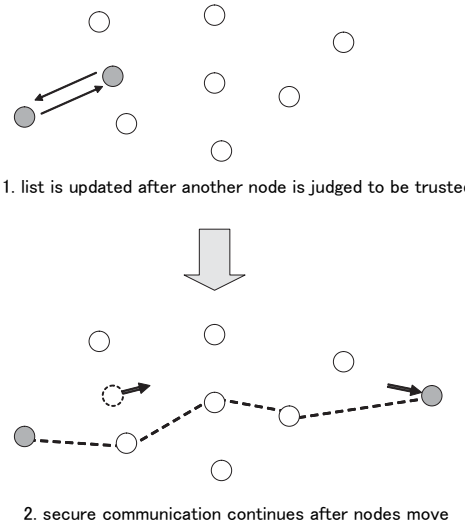

Fig. 4. Continuous secure communication

list nor belonged to the trusted group, the list is updated as follows; in this case, the most important matter is to decide if this node can be trusted. First, the nodes judge with each other if the counterpart can be trusted, when they communicate directly in MANET. Only if they are judged to be trustful with each other, the list is updated by exchanging their IDs and public keys. How to judge the credibility is not discussed in this paper – a face-to-face communication for confirmation seem to be enough in many cases. After credibility is confirmed by the direct communication, it is kept to be guaranteed even in a multi-hop communication in which untrusted relay nodes exist. This procedure is shown in Figure 4.

C. Acquisition of IP address

When a node joins MANET, this is found by the periodical routing information exchange in OLSR. As the routing table is updated at each node, a multi-hop network is configured

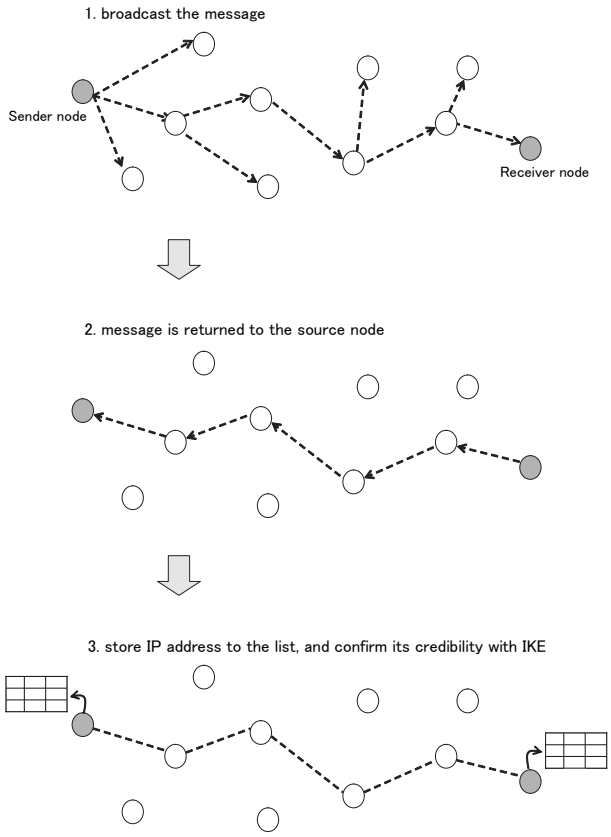

Fig. 5. Acquisition of IP address

based on the table. In MANET, since each node is distinguished by ID and address is given differently at each joined network, the destination node's ID on the list must be corresponded with its IP address. In our research work, the method of acquiring IP address is shown in Figure 5.

First, the sender node broadcasts its own ID, IP address, and the destination node's ID in MANET. Then the destination node replies its own ID and IP address to the sender when the broadcast is received. Acquired IP address is stored in the trusted nodes list as a temporarily valid address in this network. In other networks, even in a communication with the same node, IP address should be acquired again and the list must be updated.

During the IP address acquisition phase, since a message among nodes is going through unsecured connections, IP address spoofing might happen by eavesdropping and falsifying messages at relay nodes. In order to prevent these kinds of attacks, our method is making use of IKE authentication of IPsec, in which the information on the trusted nodes list is applied so that it is possible to judge whether the message is sent from the right destination node.

D. Secure connection and its reconfiguration

1) Creating a secure connection: In a multi-hop network configured with OLSR, using IP address acquired as mentioned above, communications begin with a destination node through several relay nodes. However, the communication

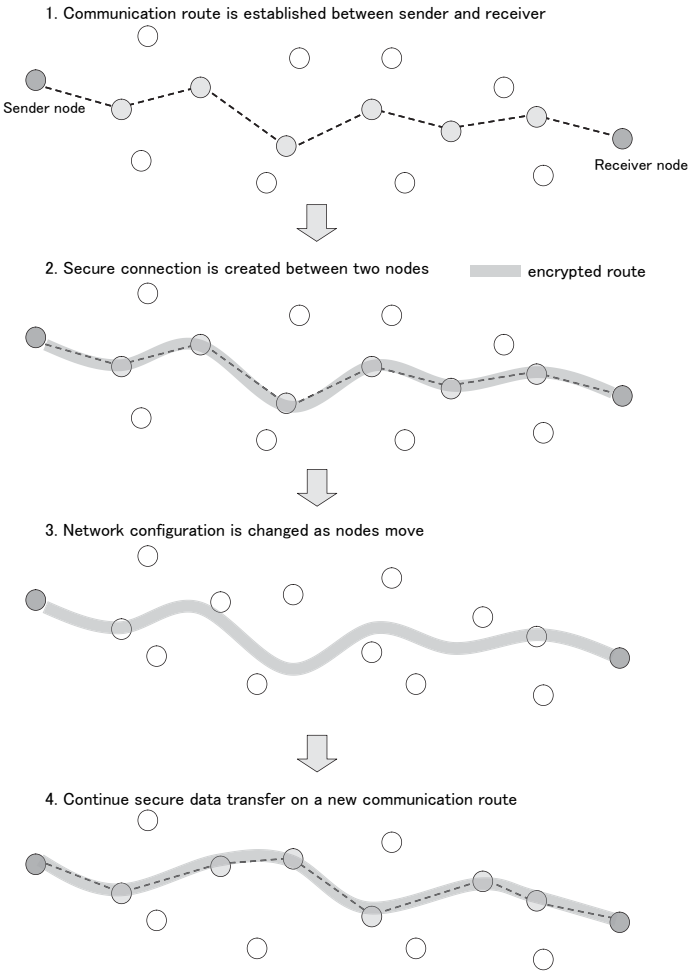

Fig. 6. Creation and reconfiguration of secure connection

is not encrypted yet in this stage. After the multi-hop route is established, the sender node creates a secure connection by making IPsec SA, which is end-to-end encryption route between the sender and the receiver. On this secure connection, because transmitted data is encrypted, relay nodes cannot look into contents even if they relay data packets.

During the phase of establishing IPsec SA, the public key on the list is used and authenticated by IKE. Thus, even if IP address falsification happens during the phase of IP address acquisition, it would be found by the IKE authentication using the public key on the list, and the spoofing would be prevented.

2) Reconfiguration of secure connection for modification of network: In the case of MANET, it is important to keep its function even if the network configuration is modified due to joining and leaving of nodes. With the proposed method, a secure connection is kept to be connected when a relay node is changed from one node to another.

As shown in Figure 6, when relay nodes move, the routing table is updated at each node and a new route from source to destination is established immediately using the information collected by OLSR. As a result, the secure connection

established on the end-to-end communication is reconfigured automatically and secure data transmission continues without noticing the change of relay nodes.

IV. Implementation and Execution of the Proposed Method

A. Experimental setup

In this paper, we have implemented the mechanism of acquiring IP address upon a request on a multi-hop network using OLSR, and creating a secure connection using this information. Moreover, we have confirmed in our experiment that a secure connection is reconfigured when a network is modified during a communication through the secure connection. In this case, all nodes on the list are assumed to be trusted.

The experimental setup is as follows; four machines are used and a multi-hop network is established as shown in Figure 7. The multi-hop network configuration will be explained in the next subsection. OLSR is used as a routing protocol, and olsrd is employed as an implementation for Linux[12]. IPsec is used for the encryption of communications, and openswan implemented for Linux is used[13]. The encryption algorithm is 3DES, security protocol is ESP, and end-to-end transport mode is chosen as a capsule method of IPsec. All machines are connected with IEEE802.11b wireless LAN, and the spec of each machine is as follows; OS: Linux2.6.9, CPU: Intel Pentium 4, Main Memory: 512Mbytes. In this experiment, node A is a sender, node C is a receiver, and nodes B and D are relay nodes joining and leaving the multi-hop network.

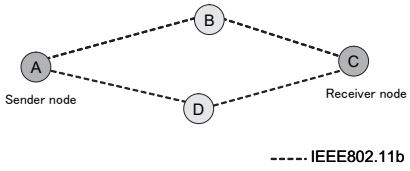

Fig. 7. Experimental setup

B. Configuration of a multi-hop network

In our experiment of a multi-hop network using OLSR, all nodes exist within a direct transmission area of wireless communication. Thus packets should be blocked to prevent direct data transmission between a sender and a receiver just for the multi-hop experiment. For example, when a multi-hop connection from node A to node C via node B is established, packets from node C should be blocked at node A and packets from node A should be blocked at node C by ”iptables” command for realization of a multi-hop communication environment.

In addition, a problem occurs such that a routing table is re-written by IPsec when an IPsec connection is created on a multi-hop route, therefore the communication is suspended because OLSR cannot correct the routing table. This is considered to be a specific problem of the implementation of openswan and/or olsrd. We have solved this problem by dropping nodes of both ends of a connection temporarily and reconnecting them again soon, so that a right routing table is generated by OLSR.

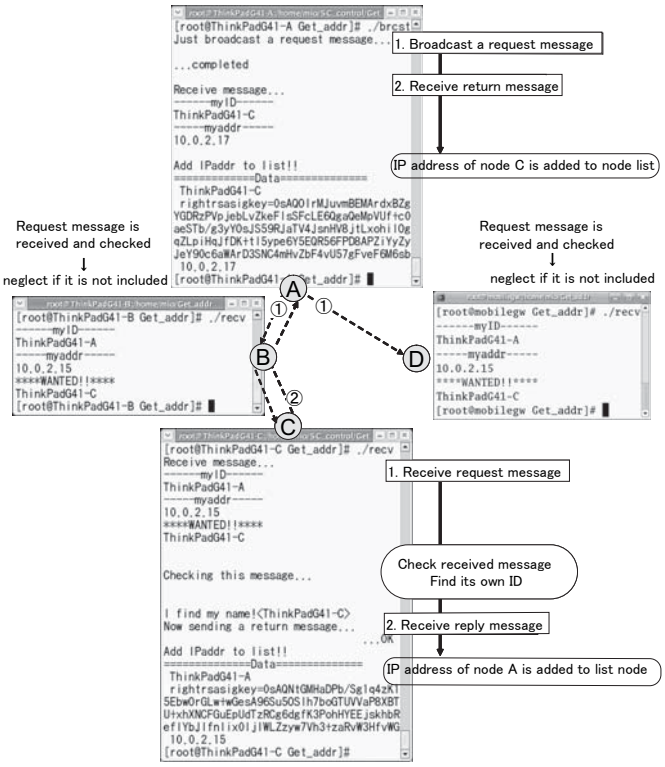

Fig. 8. Acquisition of IP address and update of the list

After a multi-hop route is created using OLSR on the above experimental environment, a secure connection is established between node A and node C, and reconfigured automatically with this management mechanism. The details of such behavior are described in the following subsection.

C. Execution of the proposed method

1) Acquisition of IP address: In order to establish a secure connection, participants in the MANET should know IP address of communication partners mutually. This is realized such that ID of each node is corresponded with IP address. First, a sender broadcast a request message including a suite of ”sender node’s ID, sender node’s IP address, destination node’s ID” in a participating network. Next, receiving nodes check the message whether its own ID is included. They neglect the message if it is not included. On the contrary, if a node confirms its own ID is included in the message, it replies a message including a pair of ”destination node’s ID, destination node’s IP address” to the sender node, and stores IP address of the sender node in its own list. Finally, when the sender node receives the reply message from the destination node, it stores IP address of the destination node in its list.

The execution of our controlling script of this procedure is shown in Figure 8. In this experiment, node A sends a request message to node B and D directly, to node C via node B

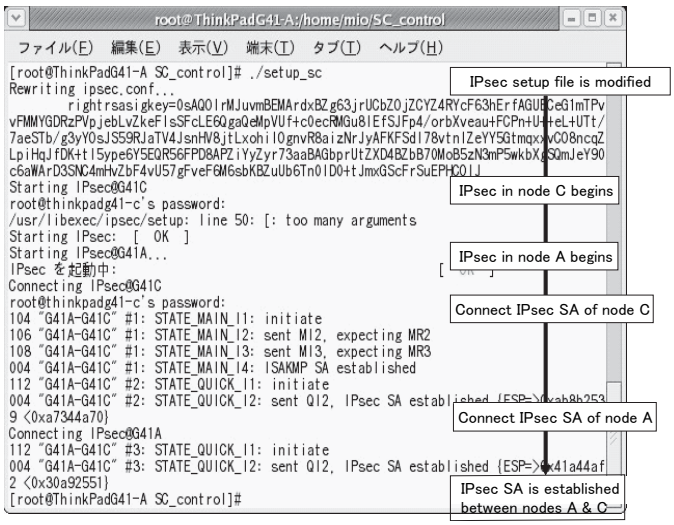

Fig. 9. Creation of a secure connection

through the route created by OLSR. The request message includes node A's ID and IP address and the destination node's ID, node C for example. When nodes B, C, and D receive and check the message, node C finds out its own ID in it. Node C replies a message including its own ID and IP address to node A, and it stores the received IP address in its list. After node A receives the reply message, it also stores the received IP address of node C in its own list.

2) Creation of a secure connection: After the procedure described in the previous subsection, nodes A and C know a public key and IP address of their counterpart with each other. When a multi-hop route is established, an IPsec setup file is modified with a public key of its counterpart at both nodes. Based on the setup file, node A begins IPsec procedure and establishes a connection so that IPsec SA connecting end-to-end of both nodes is constructed. Thus a secure connection between a sender and a receiver is created.

The procedure of creation of a secure connection is shown in Figure 9. First, the IPsec setup file is modified in both ends based on a public keys and IP addresses on the list. Next, a shared secret key using for encryption is created by IKE using the setup file. Finally a secure route is created, which provides IPsec encryption between the sender and the receiver.

3) Behavior of secure connection reconfiguration: The behavior of reconfiguration of a secure connection is confirmed, when the relay node B leaves and node D joins MANET as a relay node. In order to see the secure connection is influenced by the reconfiguration of network, transferred packets are observed on the route with "tcpdump" command while encrypted communication is performed between nodes A and C. This is shown in Figure 10.

While node B relays a communication between nodes A and C, message exchange packets of OLSR and encrypted ESP (Encapsulating Security Payload) packets of IPsec are transferred on the route. When node B drops from MANET, all communications suspend temporarily. In this case, when

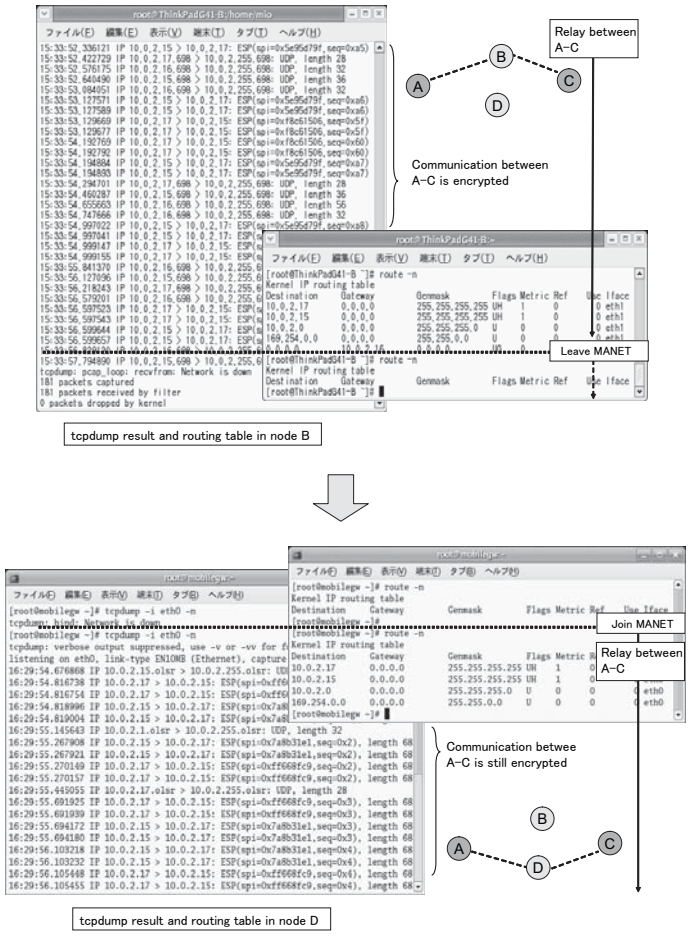

Fig. 10. Behavior of secure connection reconfiguration

node D joins the network, it works as a new relay node, and ESP packets are transferred again between nodes A and C on the route. Thus we have confirmed that the routing tables are updated by OLSR and the secure connection is reconfigured automatically. As a result, nodes A and C continue their secure communications regardless of the network configuration change.

V. Conclusions

In this paper, a model of establish and manage secure connections on a multi-hop network is proposed in order to realize secure communications on MANET. On a multi-hop environment realized based on OLSR, a control mechanism to create an encrypted route using IPsec is implemented, and it is confirmed that the route is always secure even if the network configuration is changed. As a future work, more realistic cases of multi-hop communications are discussed and the proposed model should be refined.

Acknowledgement

We would thank Prof. Hiroaki Morino in Shibaura Institute of Technology for helpful suggestions and useful discussions for the experiments of a multi-hop network.

REFERENCES

[1] MANET：http://www.ietf.org/html.charters/manet-charter.html
[2] Sye Loong Keoh and Emil Lupu: ”Towards Flexible Credential Verification in Mobile Ad-hoc Networks,” POMC 2002, 2002.
[3] Rajiv K. Nekkanti and Chung-wei Lee: ”Trust Based Adaptive On Demand Ad Hoc Routing Protocol,” ACM Southeast Regional Conference, 2004.
[4] Srdjan Capkun, Levente Buttyan, and Jean-Pierre Hubaux: ”Self-Organized Public-Key Management for Mobile Ad Hoc Networks,” ＩEEE Transactions on Mobile Computing, pp.52-64, 2003.
[5] Aruna Balasubramanian, Sumita Mishra, and Ramalingam Sridhar: ”Analysis of a Hybrid Key Management Solution for Ad hoc Networks,” IEEE Wireless Communications and Networking Conference, Vol4, pp.2082-2087, 2005.
[6] Daniele Raffo, Cedric Adjih, Thomas Clausen, and Paul Muhlethaler: ”An Advanced Signature System for OLSR,” ACM Workshop on Security of Ad Hoc and Sensor Networks, pp.10-16, 2004.
[7] Danny Dhillon, Jerry Zhu, John Richards, and Tejinder Randhawa: ”Implementation and Evaluation of and IDS to Safeguard OLSR Integrity in MANETs,” International Wireless Communications and Mobile Computing Conference (IWCMC 2006), pp.45-50, 2006.
[8] OLSR：http://hipercom.inria.fr/olsr/
[9] TBRPF：http://www.ietf.org/rfc/rfc3684.txt
[10] AODV：http://www.aodv.org/
[11] DSR：http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt
[12] olsrd：http://www.olsr.org/
[13] Linux openswan：http://www.openswan.com/