Design and Implementation of Secure Area Expansion Scheme for Public Wireless LAN Services

Ryu Watanabe  Non-member (KDDI R&D Laboratories, Inc.)
Toshiaki Tanaka  Non-member (KDDI R&D Laboratories, Inc.)

Keywords: wireless LAN, public key certificate, secure ad-hoc routing, privacy protection, DoS attack

Recently, wireless LAN (WLAN) technology has become a major wireless communication method. The communication bandwidth is increasing and speeds have attained rates exceeding 100 Mbps. Therefore WLAN technology is regarded as one of the promising communication methods for future networks. In addition, public WLAN connection services can be used in many locations. However, the number of the access points (AP) is insufficient for seamless communication and it cannot be said that users can use the service ubiquitously. An ad-hoc network style connection can be used to expand the coverage area of public WLAN services. By relaying the user messages among the user nodes, a node can obtain an Internet connection via an AP, even though the node is located outside the AP’s direct wireless connection area. Fig. 1 shows the concept of the coverage area expansion using an ad-hoc network style connection. Such a coverage area extending technology has many advantages thanks to the feature that no additional infrastructure is required. Therefore, there is a strong demand for this technology as it allows the cost-effective construction of future networks.

When a secure ad-hoc network routing protocol is used for message exchange in the WLAN service, the message routes are protected from malicious behavior such as route forging and can be maintained appropriately. To do this, however, a new node that wants to join the WLAN service has to obtain information such as the public key certificate and IP address in order to start secure ad-hoc routing. In other words, an initial setup is required for every network node to join the WLAN service properly. Ordinarily, such information should be assigned from the AP. However, new nodes cannot always contact an AP directly. Therefore, there are problems about information delivery in the initial setup of a network node. These problems originate in the multi hop connection based on the ad-hoc network routing protocol.

In order to realize an expanded area WLAN service, in this paper, the authors propose a secure public key certificate and address provision scheme during the initial setup phase on mobile nodes for the WLAN service. The proposed scheme also considers the protection of user privacy. Accordingly, none of the user nodes has to reveal their unique and persistent information to other nodes. Instead of using such information, temporary values are sent by an AP to mobile nodes and used for secure ad-hoc routing operations. Therefore, our proposed scheme prevents tracking by malicious parties by avoiding the use of unique information. Moreover, a proto system is also implemented based on the proposal. The evaluation results demonstrated the good performance of the scheme. The time required for a new node to obtain temporary information in order to join the WLAN service is approximately 780 milliseconds in our test environment. This figure is fast enough to complete the initial setup on mobile nodes. In addition, the authors describe a countermeasure against DoS attacks based on the approach to privacy protection described in our proposal.

The contributions of this paper are summarized below.

- In order to expand the coverage area of a public WLAN service, the authors propose a temporary public key certificate and address provision scheme for the operation of a secure ad-hoc routing protocol.
- By using the temporary values for the certificate and addresses instead of the persistent values, tracking actions can be blocked. Accordingly, user privacy is protected.
- By introducing the client puzzle technique on mobile nodes, DoS attacks can be eliminated.
- The prototype was implemented using a notebook PC and PDA, and the feasibility of our proposed scheme was confirmed experimentally. The results demonstrated good performance of the scheme.
Design and Implementation of Secure Area Expansion Scheme for Public Wireless LAN Services

Ryu Watanabe∗ Non-member
Toshiaki Tanaka∗ Non-member

Recently, wireless LAN (WLAN) technology has become a major wireless communication method. The communication bandwidth is increasing and speeds have attained rates exceeding 100 Mbps. Therefore, WLAN technology is regarded as one of the promising communication methods for future networks. In addition, public WLAN connection services can be used in many locations. However, the number of the access points (AP) is insufficient for seamless communication and it cannot be said that users can use the service ubiquitously. An ad-hoc network style connection can be used to expand the coverage area of a public WLAN service. By relaying the user messages among the user nodes, a node can obtain an Internet connection via an AP, even though the node is located outside the AP’s direct wireless connection area. Such a coverage area extending technology has many advantages thanks to the feature that no additional infrastructure is required. Therefore, there is a strong demand for this technology as it allows the cost-effective construction of future networks.

When a secure ad-hoc routing protocol is used for message exchange in the WLAN service, the message routes are protected from malicious behavior such as route forging and can be maintained appropriately. To do this, however, a new node that wants to join the WLAN service has to obtain information such as the public key certificate and IP address in order to start secure ad-hoc routing. In other words, an initial setup is required for every network node to join the WLAN service properly. Ordinarily, such information should be assigned from the AP. However, new nodes cannot always contact an AP directly. Therefore, there are problems about information delivery in the initial setup of a network node. These problems originate in the multi hop connection based on the ad-hoc routing protocols.

In order to realize an expanded area WLAN service, in this paper, the authors propose a secure public key certificate and address provision scheme during the initial setup phase on mobile nodes for the service. The proposed scheme also considers the protection of user privacy. Accordingly, none of the user nodes has to reveal their unique and persistent information to other nodes. Instead of using such information, temporary values are sent by an AP to mobile nodes and used for secure ad-hoc routing operations. Therefore, our proposed scheme prevents tracking by malicious parties by avoiding the use of unique information. Moreover, a test bed was also implemented based on the proposal and an evaluation was carried out in order to confirm performance. In addition, the authors describe a countermeasure against denial of service (DoS) attacks based on the approach to privacy protection described in our proposal.

Keywords: wireless LAN, public key certificate, secure ad-hoc routing, privacy protection, DoS attack

1. Introduction

Recently, there has been extremely rapid growth in wireless communication technology and wireless local area network (WLAN) has become a major method adopted by intranets or home networks. Moreover, public WLAN services have also become widespread and access points (AP) are found everywhere; for instance, airports, stations, hotels, and fast food shops. The FON service (1) is a new trend in Internet connection services using a WLAN connection. The service is based on mutual use of a user’s Internet connection. A FON user who provides his Internet connection to other FON users with his FON router (wireless LAN access point) can use other users’ Internet connections via their FON routers. In this way, the number of APs for public WLAN services is increasing steadily.

Besides the installation of the AP, an ad-hoc network style connection can be utilized to expand the coverage area of a public WLAN connection service. In an ad-hoc network, user nodes with wireless devices construct a network without any infrastructure and all nodes cooperate with each other in message exchange. By using this style of connection in WLAN services, a node can make an Internet connection via an AP, even though the node is located outside the AP’s direct wireless communication area (Fig. 1). Unfortunately, this technique has the disadvantage of causing an unstable connection due to dynamic changes in network topology resulting from the movement of network nodes. However, the service can be provided by changing the software for both AP
Secure Area Expansion Scheme for Public WLAN Services

Y. Sun et al. (2) realized this concept through cooperation between the mobile IP (3) and the ad-hoc on-demand distance vector (AODV) (4) routing protocol. However, their proposal had problems in terms of security. For example, in their proposal, a new joining node obtains an IP address without any user authentication. Moreover, the AODV routing protocol is based on cooperation and mutual trust among every ad-hoc node. All routing message are treated as genuine information. Therefore, security problems such as a routing loop or black hole attack due to a faked or forged routing message have been reported (5)-(8). Accordingly, in order to resolve security problems with ad-hoc routing protocols, many routing protocols with security functions have been proposed (7)-(9). Almost all the protocols adopt a cryptographic technique to provide security functions. For instance, secure ad-hoc routing protocols based on an asymmetric cipher algorithm use a digital signature to confirm the integrity of routing messages. The node, which receives the routing messages, validates the signature with the public key of the sender node. For this reason, in order to operate secure ad-hoc routing based on the asymmetric cipher algorithm, it is necessary to set up a public key pair. In addition, if the public key is distributed in the form of a public key certificate issued by a certificate authority (CA), each WLAN node can confirm the integrity of the public key by validating the certificate. In the case of the WLAN service described in this paper, a service provider (SP) is one candidate for the CA. If an SP has issued a public key certificate to each of its users for user authentication and provided the public key of the SP for validation of the certificate in advance, the certificate can be used for not only user authentication but also secure ad-hoc routing operation. However, in this case, the problem of user privacy arises. Protecting user privacy is one of the most important factors in mobile wireless communication. As distinct from wired connections, eavesdroppers can easily intercept the radio output from WLAN nodes. By using a secure connection like SSL, user data can be protected from eavesdropping. However, the information on routing messages cannot be protected in this way. Routing messages are exchanged in a network in order to maintain the routing path appropriately; therefore, the routing messages have to be open to everyone including eavesdroppers. If a persistent value is used for the messages, user privacy could be compromised as a result. The MAC address is one example of a persistent value on the routing message. The fact that the same MAC address is observed on different positions and different dates could reveal the movement of a user. A persistent public key certificate results in the same situation. If the same public key is used for validating the routing messages sent from the node, it could also reveal the movement of the user. These privacy problems have to be resolved for realization of the WLAN service.

Another candidate for a CA is the AP. If an AP issues a public key certificate to a new joining node, when the node joins its WLAN service, the certificates are anonymized and tracking actions from the public key are blocked. However, in this case, a problem associated with the delivery of the certificate arises. A new node does not yet have information for secure ad-hoc routing such as a public key certificate and an IP address, and the node cannot contact the AP via an ad-hoc network connection. Therefore, a solution to this problem is required in order to allow the area of the WLAN service to be expanded. In addition, in order to provide the WLAN service securely, countermeasures against malicious behaviors such as denial of service (DoS) attack are also required.

Therefore, in order to expand the WLAN service area using an ad-hoc network connection, Y. Sun’s method is insufficient, particularly with regard to security considerations. For this reason, in this paper, the authors describe a privacy enhanced coverage area expansion scheme for a WLAN service with secure ad-hoc routing. In our proposal, in order to resolve the delivery problem, the authors introduce the concept of the proxy node (PN), which helps message exchange for new joining nodes that want to join the WLAN service but have no IP address or public key certificate for secure routing operations. Our proposed scheme also considers user privacy protection. By using temporary values for the operation of the secure ad-hoc routing and message exchange, the tracking actions are thereby blocked. In addition, in our proposed scheme, in order to protect user privacy, only the AP authenticates the user. Therefore, the proxy node simply relays the request messages from the new joining node to the AP without any authentication of the messages or senders. This type of privacy-protecting rule can still leave the way open to DoS attacks. For this reason, the client puzzle technique is used on the proxy node and it contributes to reducing the number of DoS messages caused by the attack.

The contributions of this paper are summarized below.

- In order to expand the coverage area of a public...
WLAN service, the authors propose a temporary public key certificate and address provision scheme for the operation of a secure ad-hoc routing protocol.

- By using the temporary values for the certificate and addresses instead of the persistent ones, tracking actions can be blocked. Accordingly, user privacy is protected.
- By introducing the client puzzle technique on proxy nodes, DoS attacks can be eliminated.
- The prototype was implemented using a notebook PC and PDA, and the feasibility of our proposed scheme was confirmed experimentally.

2. Related Work

2.1 Area Extension of WLAN Y. Sun et al. realized the concept of extending the coverage area of WLAN services through cooperation between a mobile IP and AODV routing protocol. This proposal mainly focused on a basic scheme that allowed a mobile node to find the AP, called the foreign agent (FA), on a mobile IP scheme using the route request message of the AODV routing protocol. Security aspects are not considered. In their proposal, the IP address is allocated or determined on mobile nodes without any authentication. Therefore, malicious users can also obtain the IP address and join the ad-hoc routing. Accordingly, it is easy for them to execute malicious actions. Thus, the proposal should not be adopted for a WLAN service without some modification. Security functions are required for realization of service area extension.

The AODV (4) routing protocol is one of the ad-hoc routing protocols approved by the IETF and is categorized as an on-demand type protocol. The routing protocol is based on network nodes' cooperation and mutual trust. All the messages exchanged for route maintenance are treated as true messages. Therefore, a malicious user can easily attack the network by generating faked or forged messages. As to the IP address allocation for the AODV routing protocol, an infrastructureless system such as the zeroconf (10) is supposed to be used, instead of the dynamic host configuration protocol (DHCP). However, usually, such a system is also dependent on the honesty of every network node and is therefore associated with security problems.

2.2 Secure Ad-Hoc Routing Protocol In order to resolve security problems associated with ad-hoc routing protocols, ad-hoc routing protocols with security functions have been proposed. These protocols usually adopt cryptographic techniques for their security functions. The secure ad-hoc on-demand distance vector (SAODV) (7) routing protocol is one of the secure ad-hoc routing protocols and is based on an asymmetric cipher algorithm. A digital signature is used for validation of the routing messages and a one-way hash function protects the sequence number of the messages. In the SAODV routing protocol, the public keys have to be set up on every ad-hoc node for its operation. Regarding the address allocation, the SAODV routing protocol adopts a cryptographic generation method (13) (14) in order to confirm the validity of the message sender nodes.

In addition, there have been many studies on ad-hoc routing protocols and changes in performance due to the security functions have also been evaluated (10) (11).

2.3 Privacy Protection Privacy protection is one of the important factors in wireless communication because it is easy for anyone to listen to the wireless output from a mobile node. If unique or persistent information is used for routing messages, the user could be traced by using such information and user activity could be leaked because the routing messages have to be open to every node for route maintenance. Pseudonymization (12) is a method for user privacy enhancement and is used to block malicious actions based on traceability and linkability, which depend on the user's unique information. Instead of unique or persistent information, temporary or random information is used for communication. The MAC address (13) on network interfaces is one example of unique and persistent information. Moreover, with regard to the public key certificate used in secure ad-hoc routing, the problem is the same. If a persistent public key certificate is used for every WLAN service, the user node can be traced by using it.

2.4 Client Puzzle The client puzzle (15) technique is a countermeasure against DoS attacks. When a server gets a request from a client, then the server gives the client a puzzle before processing the request. An arithmetical problem, which is easy to formulate but hard to solve, is used for the client puzzle. The factorization of two large prime numbers is one example of how the puzzle works. For a legitimate user, to solve the puzzle requires only one trial and has low computational cost. In contrast, for the DoS attacker, solving the puzzle imposes a heavy computational load. If the attacker wants the server to process the requests, the attacker has to solve all the puzzles. Therefore, the frequency of the request is regulated and the processing cost imposed on the server is reduced as a result.

3. Proposed Scheme

In this section, the authors describe the proposed scheme. Our proposed scheme adds security functions to Y. Sun's idea. The main issue is the initial setup of the public key certificate and address for operating a secure ad-hoc routing protocol with user privacy protection. In Y. Sun's proposal, an IP address called care of address (CoA) on the mobile IP scheme is allocated to each node. In contrast, we simply employ a method similar to DHCP address allocation, because in our scheme an IP address is assigned by an AP along with a public key certificate after user authentication at the AP.

3.1 Requirements Realization of secure WLAN services with an expanded coverage area and user privacy protection using secure ad-hoc routing is our goal in this paper. The requirements for it are summarized below.

(1) User node that wants to join the WLAN service obtains the information for operating secure ad-hoc routing from an AP securely.
(2) The user node does not use persistent or unique
information for operating secure ad-hoc routing.

(3) Only the authenticated user can use the WLAN service.

The first requirement is a fundamental requirement for secure use of the WLAN service. In the supposed WLAN service, a new joining node has to operate a secure ad-hoc routing protocol for constructing the area-expanded network. For this purpose, in our proposed scheme, the node securely obtains the public key certificate and IP address from an AP.

The second requirement is the protection of user privacy. Persistent or unique information, which indicates the user or the user’s node, can be used for tracing the user. In order to block this tracking action by malicious parties, temporary information is used in our proposed scheme. Therefore, a temporary public key certificate and a temporary IP address are provided from an AP securely. In addition, a temporary MAC address is also provided from the AP simultaneously.

The third requirement is purely for security reasons. We suppose the service is provided only for the provider’s users. Therefore, the AP authenticates users before users can join its service.

3.2 Overview When a request node (here, the authors define the word request node (RN) that wants to join a WLAN service.) can contact the AP directly like a conventional WLAN service (face-to-face contact), all the messages between the RN and the AP are exchanged via a L2 connection (upper figure of Fig.2). In order to satisfy the first requirement, the node cannot announce the original MAC address of the WLAN device to the AP. Therefore, the AP sends all messages to the node in L2 broadcast form. Conversely, the RN sends messages to the AP in L2 unicast form because the AP is a part of the public infrastructure and it is not necessary to hide the AP’s MAC address for privacy protection.

Then the AP issues a temporary public key certificate and assigns an IP address and a MAC address to the RN via user authentication. Finally, the node joins the WLAN service and operates secure ad-hoc routing.

In the case where an RN cannot contact an AP directly but can contact a node which has already joined the WLAN service, our proposed scheme requires the help of secure ad-hoc routing by introducing the concept of the proxy node (PN). The PN is one of the network nodes (NN). (The authors also define the word “network node (NN)”: a node that has already joined the WLAN service using the proposed scheme and can contact the AP thanks to a secure routing path.) The PN usually acts as an NN. However, when the node receives a request message sent from an RN to the AP, the node performs the function of the PN in relation to the RN and relays the request message to the AP. In other word, the PN is a particular state of the NN. In this paper, therefore, the authors call the NN, which performs the function of the relaying messages between an RN and an AP, the PN. A PN is found and selected by an RN following the rule. First, before an RN contacts a PN, the RN sends the request message to obtain the AP’s public key certificate as an L2 broadcast message. The NN, which received the request message, sends the reply message as a response. In this case, it is possible for the RN to receive reply messages from multiple NNs. Then, the RN selects the fastest sender node as the PN for later communication after checking the reply message.

All messages between the RN and the PN are exchanged via an L2 connection (lower figure of Fig.2) as in the case where the RN and AP have a direct connection as described above. The RN node sends the request message to the PN in L2 unicast form and the PN sends the message to the RN in L2 broadcast form. The PN has already been assigned a temporary MAC address from the AP. Therefore, the PN can reveal its temporary MAC address to the RN. On the other hand, the PN and the AP can communicate with each other using secure ad-hoc routing. The PN sends the RN’s request message to the AP after encapsulating it in IP packet form. The relay message from the AP to the request node is also encapsulated as an IP packet and is then sent to the proxy node. The PN extracts the message from the IP packet and sends it to the RN in L2 broadcast form.

Once the RN has obtained the temporary values for secure ad-hoc routing from the AP, then the node can join the WLAN service and contact the AP using secure ad-hoc routing. The RN becomes an NN of the WLAN service and can communicate with the AP without the help of the PN. If the network topology changes due to movement of the network nodes, the node can find a different connection path to the AP by using secure ad-hoc routing. In addition, the node can perform the function of message proxy as a PN to new request nodes.

Instead of using the L2 broadcast in message exchange to the RN as a way of hiding the original MAC address of the RN, a random MAC address can also be used. Before sending the request messages to the WLAN service, the request node generates a 48-bit length random value and uses the value as its MAC address. This scheme has the advantage that the messages which are sent to the request node can be sent in not L2 broadcast form but
in L2 unicast form because the MAC address of the request node can be revealed without concerns regarding user privacy. However, there is a very small chance that the MAC address could be duplicated in the network. In order to avoid this problem, in the proposed scheme, the authors do not adopt the random MAC address scheme and the L2 broadcast address is utilized for sending messages from a PN to an RN.

**3.3 Network Construction** Figure 3 shows how the expanded area of a WLAN service is made possible by our proposal.

1. First, only one AP and no WLAN node is present.
2. The first RN approaches the WLAN service area and joins the WLAN service after negotiation with the AP directly.
3. Next, other RNs approach the WLAN service and join the WLAN service after negotiation with the AP directly or via the first user node as a PN depending on the nodes location.
4. The succeeding user nodes join the WLAN service in a similar way. Once an RN has joined the WLAN service and becomes an NN, the node can contact the network thanks to the secure ad-hoc routing.
5. Even if the network topology changes due to the movement of other nodes, an NN can find different routes with the help of the secure ad-hoc routing.

In step (4) and (5), a conventional secure ad-hoc routing protocol is supposed to be used. For instance, in case of the SAODV, an NN finds a route following the manner described below. When the right edge NN in Fig. 3-(4) wants to find the route for the AP, the node makes a route request message targeting the AP and sends it as a broadcast message. The neighbor node, which receives the message, rebroadcasts it and memorizes the address of the previous hop for building the routing table. Finally, the message reaches the AP through the rebroadcasting. Then the AP generates the reply message and returns it as a unicast message. Each intermediate NN sends the reply message to the memorized address as a unicast message. By this process, each NN builds the routing table and the route from the right edge NN to the AP is achieved as a result. In order to confirm the message legitimacy, all messages are signed at the source NN and validated at the receiving NNs. In order to avoid resending the same request messages, the sequence number is used. A receiving NN checks the number if the NN has received the request message targeting the same destination previously. If the number is no less than the previous one, then the NN stops rebroadcasting it. Therefore, usually, the shortest (the minimum hops) path is identified.

The proposed scheme follows the same rule of the original SAODV protocol in order to reroute the routing path on the service (Fig. 3-(5)). If a lost link is detected by neighbor NNs, then they eliminate the tables concerned to the lost link. If an NN wants to recover the route including the lost link, the NN seeks another route in the same manner mentioned above.

**3.4 Client Puzzle** As the authors mentioned before, in our proposed scheme, only the AP authenticates users of new joining nodes to the WLAN service and all the request messages are relayed to the AP via proxy nodes. The AP can reject these requests through user authentication if the request messages are sent from illicit users. However, the request messages are exchanged between the proxy nodes and the AP. As a result, the wireless bandwidth is consumed and the DoS attacks thus have an adverse effect. In order to resolve this problem, in our scheme, the client puzzle technique is adopted. By using the technique at the proxy node, the frequency of DoS attack messages, which pretends to be request messages, sent to the AP is regulated. Accordingly, a DoS attack dose not work effectively. The authors assume that the client puzzle is not always used on the PN. For instance, the network node monitors the frequency of the request messages in our proposed scheme. When the node detects a number of requests that greatly exceeds the threshold, then the node implements a client puzzle for a specified period.

**3.5 Security Model** Before describing the sequence in detail, the security model of the supposed WLAN service is described below and the symbols used in the following explanations are listed in the table 1 and Fig. 4 shows the service image of the WLAN service in our proposed scheme.

- Both SP and APs are fully trusted and they do not
take any malicious actions.
• The WLAN service is provided by an SP only to the SP’s users.
• The SP provides its own public key ($PK_{SP}$) to the SP’s users (Fig. 4-(A)). The authors suppose that users can easily confirm the validity of the SP’s public key ($PK_{SP}$). For instance, the public key certificate is issued by a major trusted third party (Fig. 4-(B)) and the SP sends the certificate to its users.
• The SP issues public key certificates ($Cert_{SP}(PK_{AP})$) to every AP (Fig. 4-(C)).
• The users retain information for user authentication such as ID / password, token, IC card, etc. (Any authentication method can be adopted for our proposed scheme. In the explanation and implementation presented in this paper, the public key certificate is provided as a sample case. Therefore, the SP issues every user with a public key certificate ($Cert_{SP}(PK_{U})$) (Fig. 4-(D)) and the APs also hold a public key of the SP ($PK_{SP}$) (Fig. 4-(E))
• The users can validate the AP’s public key certificate issued by the SP ($Cert_{SP}(PK_{AP})$) using the AP’s public key ($PK_{AP}$). The APs can also validate users public key certificates issued by the SP ($Cert_{SP}(PK_{U})$) for user authentication.
• Each AP can issue a temporary public key certificate ($Cert_{AP}(PK_{NN})$) to the network nodes signing with its own private key ($SK_{AP}$).
• User nodes can validate the temporary public key certificate issued to the user network node ($Cert_{AP}(PK_{NN})$) using the AP’s public key ($PK_{AP}$) on the public key certificate ($Cert_{SP}(PK_{AP})$) issued by the SP.
• The message routing path in the WLAN services is maintained by a secure ad-hoc routing protocol based on an asymmetric cipher algorithm.

3.6 Sequence Details Here, the authors describe the procedure of providing a temporary user public key certificate and addresses by an AP. The sequence of the proposed scheme comprises two phases. In the first phase, a request node searches for the AP public key certificate using the AP’s public key certificate ($Cert_{SP}(PK_{AP})$). The public key ($PK_{AP}$) is used for encryption of the request messages in the second phase. In the second phase, the request node obtains a temporary public key certificate and addresses from the AP.

(A) First phase:
The left figure of the Fig. 5 shows the sequence of the first phase.
(1) An RN sends the request message searching for the AP’s certificate ($Cert_{SP}(PK_{AP})$) in the form of an L2 broadcast message.
(2) An NN, which received the (A)-1 request message, sends the reply message with the AP’s public key certificate ($Cert_{SP}(PK_{AP})$), which the NN already has, as an L2 broadcast message. In this step, the AP also behaves in the same manner. Therefore, if the AP receives the request message, then the AP sends the reply messages with its own public key certificate.
(3) When the RN receives the L2 broadcast message as a reply message, the RN records the source MAC address of the message because the sender NN will be utilized as the RN for the RN in the second phase. Therefore, this MAC address is used as the destination address of the L2 unicast messages sent from the RN in the B-(2) and (6).
In this step, there is the possibility that the RN could get multiple reply messages from multiple NNs. In this case, the RN stores all the messages and records the source MAC addresses. If the RN gets no reply in this step, then the RN moves and sends the request message again.
(4) The RN validates the certificate ($Cert_{SP}(PK_{AP})$) on the reply message after receiving it. If the validation succeeds, the node has received a valid certificate of the AP and can use the AP’s public key ($PK_{AP}$) in the certificate. If the validation fails, then the request node checks the other reply messages in order of arrival until the validation...
 succeeds or the reply messages run out. By this process, the RN selects the first valid certificate sender NN as the PN for the next phase. If the RN gets no valid certificate in this step, then the RN moves and sends the request message again.

(B) Second phase:

The right figure of Fig. 5 illustrates message exchange in the second phase. Fig. 5-(α) shows the three basic nodes connection set-up of RN-PN-AP. However, the connection between an RN and an AP depends on the network topology. If an RN makes contact with an AP directly, the messages are exchanged between them without the help of a PN (Fig. 5-(β)). The routing path between a PN and an AP is maintained by secure ad-hoc routing, therefore, there is no limitation in terms of the number of the network nodes on the routing path between a PN and an AP (Fig. 5-(γ)). In any case, the messages exchanged between an RN and an AP are the same. The following explanations are provided along with the case shown in Fig. 5-(α).

1. The RN, which has obtained the AP’s public key certificate (Cert<sub>AP</sub>(PK<sub>AP</sub>)) in the previous phase, prepares a new public key pair (PK<sub>RN</sub>, SK<sub>RN</sub>). This is then used for secure ad-hoc routing later. The node also generates a random number as a nonce (nonce<sub>AP</sub>).
2. Then the RN sends the first request message to the AP. The node encrypts the public key (PK<sub>RN</sub>) and the nonce (nonce<sub>AP</sub>) with the public key of the AP (PK<sub>AP</sub>) and sends it to the PN, which has given the AP information to the RN as an L2 unicast message by using the PN’s MAC address (MAC<sub>PN</sub>) as the destination address.
3. The PN relays the request message to the AP using secure ad-hoc routing. All the messages, which are exchanged between the RN and the AP, are relayed via this PN.
4. The AP decrypts the request message with its own private key (SK<sub>AP</sub>) and gets the temporary public key of the node (PK<sub>RN</sub>) and the nonce (nonce<sub>AP</sub>). Then the AP also generates a random number as a nonce (nonce<sub>AP</sub>). Both nonces are sent back to the RN encrypted with the RN’s public key (PK<sub>RN</sub>).
5. The PN relays the message to the RN as an L2 broadcast message.
(6) The RN decrypts the message with its own private key ($SK_{RN}$) and confirms the nonce ($nonce_{RN}$) that the request node sent at (B)-2. Then the node prepares to send the second request message. The node sends the message part consisting of the nonce ($nonce_{AP}$), which was sent from the AP, and the user public key certificate issued by the SP ($Cert_{SP}(PK_{U})$) and generates a digital signature ($Sig_{SK_{U}}$) with the private key ($SK_{U}$), which responds to the user public key ($PK_{U}$). The message part and the signature are encrypted with the AP’s public key ($PK_{AP}$). Finally, the RN sends the message to the AP via the PN.

(7) The AP decrypts the message with its own private key ($SK_{AP}$) and confirms the nonce ($nonce_{AP}$), which the AP sent in a previous message, and validates the user public key certificate ($Cert_{SP}(PK_{U})$) and checks the signature ($Sig_{SK_{U}}$) for user authentication. Next, the AP prepares addresses ($MAC_{RN}, IP_{RN}$) assigned to the node and issues the public key certificate ($Cert_{AP}(PK_{RN})$) to the user’s temporary public key. Both addresses and certificate are encrypted with the RN’s temporary public key ($PK_{RN}$) and sent to the RN via the PN.

(8) Finally, the RN obtains a temporary public key certificate ($Cert_{AP}(PK_{RN})$) and temporary addresses ($MAC_{RN}, IP_{RN}$) by decrypting the second message from the AP.

Upon completion of this sequence, the RN has finished preparation for starting secure ad-hoc routing and joining the WLAN service.

3.6.1 Client Puzzle Where a client puzzle is used on a PN, the sequence described above is slightly modified as described below.

(1) A PN informs the RN that a client puzzle is being sent in the next sequence, in the (A)-3 reply message.

(2) The RN sends a puzzle request message to the PN with the RN’s public key ($PK_{RN}$) to the RN as an L2 unicast message.

(3) The PN generates a client puzzle and sends the puzzle encrypted with the RN’s public key ($PK_{RN}$) as an L2 broadcast message.

(4) The RN decrypts the message and calculates the answer to the puzzle. Then the node sends the answer with the digital signature signed by its own private key ($SK_{RN}$) to the PN.

(5) If the signature is valid and the answer is correct, then the PN sends permission to the RN. Consequently, the second phase starts.

3.7 Security Analysis

3.7.1 Privacy Protection An RN can hide its MAC address and the temporary public key certificates are used for secure ad-hoc routing. Therefore, no nodes provide unique or persistent information to others in the proposed sequence. As a result, no one can trace the node by using the information, thereby protecting the privacy of the user.

3.7.2 Message Exchange All the messages exchanged between an RN and an AP via a PN are respectively encrypted by their own public keys; therefore, the eavesdropper, including the PN, cannot know the contents of all the messages exchanged in our scheme.

3.7.3 Mutual Authentication An AP authenticates the user of an RN by validating the user certificate with the SP’s public key and the user authenticates the AP by validating the signature of the temporary certificate with the AP’s public key certificate issued by the SP. No other party can impersonate both user and AP. Thus, a man-in-the-middle type attack is prevented. In addition, the AP assigns IP and MAC addresses based on the user authentication. Therefore, the AP can reject a subsequent request from the same user node by checking the records. Accordingly, a node cannot have more than two legitimate addresses and certificates.

3.7.4 Replay Attack An RN and an AP exchange nonces in the proposed sequence. Therefore, malicious users cannot reuse the messages sent from both the RN and the AP in the previous session.

3.7.5 Temporary Public Key Certificate In the proposed scheme, the lifetime of the temporary public key certificate is limited to such a short time that no one can break the public key pair. Therefore, the proposed scheme does not require a certificate revocation list (CRL) or online certificate state protocol (OCSP) in order to validate the certificate. Each network node only has to check the lifetime of the certificate and validates the signature on it using the AP’s public key. If an NN wants to remain in the WLAN service over the lifetime of the certificate, then the NN sends the update request message to the AP before the certificate expires. The AP reissues the new temporary public key certificate to the NN following the request.

In addition, the certificate retains the relationship between the public key and the IP / MAC addresses for the NN. For instance, both addresses are credited on the common name field of the certificate when it is issued by the AP. Therefore, NNs can confirm the validity of the sender IP address of the routing messages by checking the sender’s public key certificate.

3.8 Comparison Table 2 shows a comparison between our proposed scheme and Y. Sun’s scheme. The security features are supported in our proposal. Therefore, our proposed scheme can more realistically be employed to realize a secure WLAN service by using an ad-hoc network style connection.

4. Implementation

In order to evaluate the feasibility of our proposed scheme, the authors set up a test bed with notebook PCs and carried out performance tests. Table 3 shows the specs of the notebook PCs which were used for the evaluation. The system configuration is shown in Table 4. The modules for request node, proxy node, and AP were implemented as JAVA applications. For the wireless communication, an 802.11b type Wireless LAN system was used and operated in an ad-hoc mode. The function point metrics of both modules are 112 for the
The SAODV routing protocol was used as the secure routing protocol for our implementation. We chose it as it is one of the main secure ad-hoc routing protocols based on an asymmetric cipher algorithm and a source code (A-SAODV (17)) is provided. For the implementation, the authors slightly modified the A-SAODV routing protocol. In the original SAODV routing protocol, the public key is only used for routing message validation. In contrast, in our proposed scheme, in order to able to confirm the integrity of the public key, the public key takes the form of the public key certificate and the AP issues the certificate. Therefore, the public key used to validate the signature of routing messages is derived from the certificate at the receiving node after validating it with the AP’s public key issued by the SP. This is the main modification of the SAODV routing protocol in our implementation.

4.1 Client Puzzle A one-way hash function was used for the client puzzle on a proxy node. When a proxy node receives a request message from the request node, the proxy node generates N pieces of bit string $S_i (i = 1, 2, \cdots, N)$ of length L and calculates the $H_i (= SHA-1$ hashed value of the $S_i$). Then the node sends the $\{N, L, H_i (i = 1, 2, \cdots, N)\}$ to the request node as a client puzzle. The request node tries to find the answer to the puzzle $S'_i$ which satisfies $H'_i = hash(S'_i (i = 1, 2, \cdots, N))$ by conducting an exhaustive search. In this implementation, SHA-1 was used as a one-way hash function.

4.2 Implementation on PDA In order to confirm the flexibility of the proposed scheme, the authors implemented the proposed scheme on a device with a lower power CPU than a notebook PC. The authors used a PDA (Personal Digital Assistant) as the request node. The specification of the PDA is shown in Table 5.

5. Evaluation

In order to evaluate the basic performance of the proposed scheme, we measured the time taken by a request node to obtain addresses and a certificate from the AP. Our test bed consisted of three nodes: a request node, proxy node, and AP. Fig. 6 shows the network topology. The evaluations were carried out in-house, therefore, in order to realize a multi hop environment where the RN and the AP cannot directly contact each other, the specific packets were filtered out based on the source addresses at the RN and the AP.

5.1 Performance without Client Puzzle Table 6 shows the evaluation results for operation time. All values are the averaged values of twenty trials. From this evaluation, it was confirmed that the time taken for obtaining an address and certificate was 721 milliseconds. In addition, it took approximately 60 milliseconds to start secure ad-hoc routing from the node that had obtained the addresses and a certificate. Therefore, the total time from sending the request until joining an ad-hoc network was approximately 780 milliseconds in this test environment. Fig. 7 shows the peak CPU load of the PN and the AP of the trials. The solid marks represent the averaged values of twenty trials. It was confirmed that the peak CPU loads are approximately 25 % and 45 % on the PN and the AP, respectively.

Therefore, one operation of our proposed scheme is finished in a short time and the level of CPU utilization is not high on either the PN or the AP. In addition, the frequency of this initial operation is not high because an RN performs the operation only once before joining the WLAN service. Consequently, the total load imposed on the PN and the AP is reduced to low level. Therefore, our proposed scheme hardly affects the performance of the ordinary routing in the WLAN service.

5.2 Performance with Client Puzzle

5.2.1 Effect on Request Node To evaluate the effect of the client puzzle on the request node, the time required to find the answer to a puzzle was measured. In order to suppress the dispersion of the values, one client puzzle consisted of three questions. Fig. 8 shows the evaluation results. Fifteen trials were carried out for

### Table 2. Comparison

<table>
<thead>
<tr>
<th>Concept</th>
<th>V. Sun’s scheme</th>
<th>Proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad-hoc routing</td>
<td>AODV</td>
<td>Secure ad-hoc routing protocol based on asymmetric cipher algorithm</td>
</tr>
<tr>
<td>Security features</td>
<td>N/A</td>
<td>Any</td>
</tr>
<tr>
<td>User authentication</td>
<td>N/A</td>
<td>Client puzzle</td>
</tr>
<tr>
<td>Privacy protection</td>
<td>N/A</td>
<td>Secure routing protocol</td>
</tr>
</tbody>
</table>

### Table 3. Specifications of notebook PC

<table>
<thead>
<tr>
<th>CPU</th>
<th>Intel Pentium M (1 GHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>512 MByte</td>
</tr>
<tr>
<td>WLAN</td>
<td>802.11b</td>
</tr>
</tbody>
</table>

### Table 4. System configuration

<table>
<thead>
<tr>
<th>OS</th>
<th>Fedora Core 4 (kernel 2.6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption algorithm</td>
<td>RSA (key length 1024 bit)</td>
</tr>
<tr>
<td>Signature algorithm</td>
<td>RSA (key length 1024 bit)</td>
</tr>
<tr>
<td>One-way hash function</td>
<td>SHA-1</td>
</tr>
<tr>
<td>Cryptography library</td>
<td>OpenSSL Version 0.9.7</td>
</tr>
<tr>
<td>SAODV</td>
<td>A-SAODV Version 0.2</td>
</tr>
</tbody>
</table>

### Table 5. Specifications of PDA

<table>
<thead>
<tr>
<th>CPU</th>
<th>PXA255 (400MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>64 MByte SDRAM</td>
</tr>
<tr>
<td>WLAN</td>
<td>802.11b (CF card type)</td>
</tr>
</tbody>
</table>

Fig. 6. Test environment
Table 6. Evaluation result without client puzzle

<table>
<thead>
<tr>
<th>Message exchange for addresses and certificate</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1 Request Node</td>
<td>22 mSec</td>
</tr>
<tr>
<td>Phase 1 Proxy Node</td>
<td>214 mSec</td>
</tr>
<tr>
<td>Phase 1 Access Point</td>
<td>18.3 mSec</td>
</tr>
<tr>
<td>Others</td>
<td>83.7 mSec</td>
</tr>
<tr>
<td>Sub total</td>
<td>721 mSec</td>
</tr>
<tr>
<td>LAN device reconfiguration Request Node</td>
<td>9.2 mSec</td>
</tr>
<tr>
<td>Start routing Request Node</td>
<td>49.2 mSec</td>
</tr>
<tr>
<td>Sub total</td>
<td>58.4 mSec</td>
</tr>
<tr>
<td>Total</td>
<td>779 mSec</td>
</tr>
</tbody>
</table>

*:Reconfiguration without device up/down

Fig. 7. Evaluation result of CPU load

Fig. 8. Evaluation result of client puzzle on request node

The evaluation results in such a situation. In this evaluation, the request node, which pretended to be a DoS attacker, sent request messages to the proxy node continuously and repeated the process for obtaining addresses and a certificate. When the client puzzle was sent from the proxy node, the request node solved the puzzle and continued the request sequence. The bars in Fig. 9 represent the number of packets sent during a 10-minutes monitoring period. It was confirmed that the number of exchanged packets decreased as the puzzle length got longer. This is because the frequency of sending messages was regulated by the client puzzle. In the measurement using a 22-bit length client puzzle, the number of total packets was suppressed to less than 10% compared to the case without a client puzzle. Therefore, the use of a client puzzle at proxy nodes more effectively contributes to reducing the number of messages exchanged in the network than when it is used at an AP only. Fig.10 and Fig.11 show the change in the CPU utilization rate during the evaluation. By comparing these figures, it can be confirmed that the CPU utilization rate is greatly improved on both the PN and the AP thanks to the reduction in the frequency of message exchanges between the PN and the AP using the client puzzle technique at the PN. The peaks on the Fig. 11 represent the CPU load for the processing of the request messages between the PN and AP after the attacker node submits the correct answer to the puzzle. Table 7 summarizes the average CPU utilization rate in each experiment. In the case of the 22-bit puzzle, the average CPU rates at the PN and the AP are reduced to the approximately one fifth and less than one seventh as compared to the case where no client puzzle is used, respectively.

In a practical environment, however, an AP and NNs have other tasks such as ordinary message routing for other NNs. In addition, the machine specs are different and varied. Therefore, the appropriate length of the client puzzle cannot be fixed unequivocally. In our implementation, however, the length of the puzzle can be adjusted. Therefore, if a WLAN service is subjected to a severe attack, the service can correspond to it by flexibly extending the length of the puzzle.

While an attacker can send DoS messages directly to an AP, the attacker has to solve the puzzle. Fig. 9 shows the time required to solve the puzzle. From the evaluation, it was confirmed that it took approximately 100 seconds to answer a puzzle with three pieces having a puzzle length of 24 bits. At the time of measurement, the CPU utilization rate was monitored by system command and it was confirmed that the rate was 100% while the node was solving a puzzle.

5.2.2 Effect on Network

To evaluate the benefits of the client puzzle for the network, the number of packets exchanged among network nodes and the AP was counted using a node log-file and packet capture tool. The test environment was the same as that used for the basic performance evaluation.

If a DoS attacker does not attempt to solve the puzzle, all DoS attack messages are stopped at the PN and no messages are relayed to the AP. Accordingly, a DoS attack against the AP will fail. By repeating the sending of messages to a PN, the DoS attack against the PN will succeed. However, the operations at the PN, which performs the client puzzle, are merely receiving and rejecting the messages and they do not impose a heavy computational load on the PN. Even if a PN becomes disabled by DoS attacks, RNs can find other PNs depending on the nodes’ location and the network topology. As a result, the damage to the network is limited.

If a DoS attacker wants to send DoS messages to an AP, the attacker has to solve the puzzle. Fig. 9 shows
client puzzle. (This is the ordinary use of the client puzzle technique.) As a result, the DoS attack does not work effectively.

5.3 PDA The time required to obtain addresses and a certificate and the time taken to solve the client puzzle were measured. The evaluation settings were same as those used in the case of the notebook PC. The only difference was that the device for the request node was replaced by the PDA. Fig. 12 and Fig. 13 show the results. The results for the notebook PC are also shown for comparison. From the evaluation, it was confirmed that the processing time on the PDA was approximately three and a half times longer compared to the case of the notebook PC. The total time for getting addresses and a temporary certificate was less than one and half seconds. This is longer than the time taken when the notebook PC was used. However, it is not particularly long compared to other initial setup methods for joining a network such as an address configuration process like DHCP. Therefore, the authors thought the time was not excessively long and would be acceptable to users. From the evaluations with both the notebook PC and PDA, it was confirmed that the processing time at the request node for obtaining a certificate and addresses is roughly proportional to the CPU power of the node. This fact will assist in the setting up of a rough standard for designing a system for mobile nodes with different CPU power such as mobile cellular phones.

6. Conclusion

In this paper, the authors proposed an initial setup scheme to expand the coverage area of a WLAN service with secure ad-hoc routing. In our proposed scheme, a temporary public key certificate and IP and MAC addresses for secure ad-hoc routing are provided from an AP. In addition, user nodes do not have to provide unique information in the process employed by the proposed scheme. These features prevent others from tracking the user by using unique information. As a result, user privacy can be protected. The performance evaluation results indicate good performance. Even in the case of a PDA, the time taken to obtain a certificate and addresses is relatively short at less than one and half seconds. As a measure against DoS attacks, the client puzzle technique is used on the proxy nodes. It shows more effective performance than when it is used on the AP only. The implementation and evaluations of the proposed scheme are of great value because studies about secure ad-hoc networks and routings investigated using computer simulations and real implementations are rare. Therefore, the authors believe that this paper contributes to the realization of secure and convenient WLAN services.

(Manuscript received Jan. 25, 2008, revised April 16, 2008)
Secure Area Expansion Scheme for Public WLAN Services

References

(1) FON: http://www.fon.com/
(17) A-SAODV: http://saodv.cifriel.it/

Ryu Watanabe (Non-member) received the B.E. and M.E. degrees of Electronic Engineering from the University of Tokyo, Japan in 1997 and 1999, respectively. He joined KDD (now KDDI), and has been engaged in research on optical network, network security, mobile network security, and identity management technique. He is currently the research engineer of the Information Security Laboratory in KDDI R&D Laboratories, Inc. He is a member of IEICE.

Toshiaki Tanaka (Non-member) received the B.E. and M.E. degrees of Communication Engineering from Osaka University, Japan, in 1984 and 1986 respectively. He joined KDD (now KDDI), and has been engaged in research on network security, cryptographic protocol, mobile security, digital rights management, and intrusion detection techniques. He is currently the leader of the Information Security Laboratory in KDDI R&D Laboratories, Inc. He received his doctorate of engineering from Kyushu University in 2007. He is a member of IPSJ.