IEICE TRANS. COMMUN., VOL.E88–B, NO.6 JUNE 2005

PAPER

ISMANET: A Secure Routing Protocol Using Identity-Based Signcryption Scheme for Mobile Ad-Hoc Networks*

Bok-Nyong PARK[†], ***Student Member and*** **Wonjun LEE**[†a)], ***Member***

SUMMARY Mobile ad-hoc networks consist of mobile nodes interconnected by multihop path that has no fixed network infrastructure support. Due to the limited bandwidth and resource, and also the frequent changes in topologies, ad-hoc network should consider these features for the provision of security. We present a secure routing protocol based on identity-based signcryption scheme. Since the proposed protocol uses an identity-based cryptosystem, it does not need to maintain a public key directory and to exchange any certificate. In addition, the signcyption scheme simultaneously fulfills both the functions of digital signature and encryption. Therefore, our protocol can give savings in computation cost and have less amount of overhead than the other protocols based on RSA because it uses identity-based signcryption with pairing on elliptic curve. The effectiveness of our protocol is illustrated by simulations conducted using ns-2.

key words: *ad-hoc networks, secure routing, identity-based signcryption*

1. Introduction

With the popularization of the Internet and the evolution of wireless technologies, the use of mobile computing for various kinds of the Internet applications has increased significantly in recent years. Ad-hoc network, one of the most popular techniques to support this trend, is a temporal network in which mobile nodes with wireless interface dynamically establish connection without preexisting communication infrastructure [14]. Such networks can be very useful in crucial and vital applications such as the military operations in enemy battlefield, emergencies, and rescue operations. However, the communication connection in ad-hoc network has many weakness points. For example, although there are some routes between mobile nodes, it is possible to happen that all routes are disconnected due to the mobility of nodes. To provide the mobility of nodes, ad-hoc network should not waste the time and resources for the computation and modification of routing. IETF MANET (Mobile Ad-Hoc Networks) Working Group has focused on the study of routing protocols because the optimized routing protocols are required for the efficient communication between nodes.

Most of proposed routing protocols for ad-hoc network are optimized for performance in dynamic environment. However, many of these routing protocols have security vulnerabilities from attacks. Moreover, the security of ad-hoc network is more vulnerable than that of wireless networks using fixed infrastructure, so that the security services in the ad-hoc network faces a set of challenges [14]. Ad-hoc network security research often focuses on secure routing protocols. However, such routing protocols neglect the inheritance feature of ad-hoc network such as resource-constrained in bandwidth, limited processing and memory capacity, low energy, and so on [1]. In this paper, our fundamental goal is to provide a low overhead, fast computational time, and secure routing in ad-hoc network. To improve the efficiency of computation, the proposed protocol, named ISMANET (Identity-based Signcryption scheme for MANET), uses the authentication algorithms based on the identity-based signcryption scheme [3]. It uses bilinear maps (the Weil pairing) over elliptic curves [7]. The identity-based cryptosystem has some advantages that it does not need to authenticate a public key certificate and also to maintain a public key directory. The signcryption scheme can carry out both encryption function and signature function at one time [18]. Therefore, ISMANET can guarantee the efficiency of computation and communication. Moreover, it can reduce the load of computation and reply faster because it operates over elliptic curves [9].

This paper is organized as follows. Section 2 overviews the security in ad-hoc network and Sect. 3 briefly reviews protocol and key distribution mechanism. Section 4 explains the secure routing protocol which uses identity-based signcryption scheme and Sect. 5 proofs correctness of our protocol. Section 6 shows simulation results and Sect. 7 discusses performance analysis. Finally, Sect. 8 concludes the paper. The appendix presents a formal analysis of the ISMANET.

2. Related Work

The ad-hoc network is particularly vulnerable due to its fundamental characteristics of resource-constrained, limited processing and capability, dynamic topology, and absence of central authorities. In other word, they are exposed in many dangers. Especially, control messages of routing protocol can cause serious problems because they are usually broadcasted. The studies of secure routing in ad-hoc network have been carried out by ARAN [2], Ariadne [17], SRP [15], and so on [12]. ARAN [2] protocol consists of a preliminary certification process, a mandatory end-to-end authentication stage, and an optional second stage that provides secure shortest paths. Fundamentally, it requires the use of a trusted certificate server because each node has to request a certificate signed by a trusted certificate server be-

Manuscript received March 17, 2004.
Manuscript revised August 11, 2004.

[†]The authors are with Department of Computer Science and Engineering, Korea University, Korea.

*This work was supported by Korea Research Foundation Grant (KRF-2003-041-D00509).

a) E-mail: wlee@korea.ac.kr

DOI: 10.1093/ietcom/e88–b.6.2548

fore entering the ad-hoc network. However, it has a serious problem of high overhead to sign and verify the message. Ariadne [17] protocol is an on-demand secure ad-hoc routing protocol based on DSR that withstands node compromise and relies on only highly efficient symmetric cryptography like hash function. This protocol can reduce the computation of cryptography due to the use of TESLA authentication protocol which is secret key cryptography using both hash chain and time synchronization but it has a problem that it must have all information of discovery routing paths. SRP [15] provides correct routing information. The requirement of SRP is that any two nodes have a security association. However, the most serious problem in SRP is that it cannot provide authentication process for the intermediate nodes between the source node and the destination node.

3. Preliminaries

In this section, we briefly review the protocol scenario and key distribution mechanism.

3.1 Overview of the Protocol

The routing protocol chosen for proposed protocol is AODV [6]. Thus, our protocol retains most of the AODV mechanisms. The operation of the protocol can be divided into route discovery and route maintenance process.

Whenever the route from a source node 'S' to a destination node 'D' needs to be found, the route discovery process is initiated. Route requests are broadcasted and propagated through the network. When the destination or an intermediate node with route to the destination receives the route request, it sends back a route reply to the initiator of the route request. The control messages sent during route discovery process are responsible for updating the route table of the source, the destination and all intermediate nodes. The messages, therefore, must be authenticated. In order to prevent external attacks, we have proposed a secure routing protocol, named ISMANET, based on identity-based signcryption scheme. Our protocol is based on the following assumptions:

- ARAN [2] protocol defines a set of three discrete ahhoc networks environments: open, managed open, and managed-hostile. The proposed protocol is satisfied in the managed-open environment.
- The problem of compromised nodes is handled by mutual suspicion among the mobile nodes. If nodes detect and confirm a compromised node, the compromised node is isolated by the other nodes. This approach is based on the model presented by [11]. In this paper, however, we will not take up this matter in detail.
- The nodes have enough power energy and computationally powerful enough to execute our protocol.
- All links between the nodes are bi-directional.

3.2 Key Distribution

In this subsection, we describe the key distribution mechanism for our scheme. These keys are essential for the functioning of ISMANET. Since ad-hoc network does not have a central control, key management and key distribution are challenging issues [1], [11], [12]. There are interesting issues, but they are not our major topics.

- At the time of network formation, the nodes that are forming the network decide on a mutually acceptable set of security parameters. All nodes keep the security parameters which are G_1, G_2, e, P, $P_{pub} = SK^*.P$, where SK^* is system master secret key, and include a threshold t of key service nodes. The participating nodes generate a system master public key PK^* for an identity-based signcryption scheme. It is created in a distributed fashion. The system master secret key SK^* will be shared in a $(n, t+1)$ threshold manner by this initial set of n nodes. The system master public key is distributed throughput the network and assumed to be known by everyone. Once this system master public key is established, identities may be used as public keys. The personal private key corresponding to their public key is obtained by $SK_{node} = SK^*.PK_{node} = SK^*.Hash(ID_{node})$.
- Whenever, two nodes desire to communicate to each other, they do not need the certificate exchange but they will use the public key generated from the sender's ID to verify the received signature. The public keys are exchanged when two nodes interact for the first time. The nodes can then mutually authenticate one another using their individual public/private keys and security parameters.
- In this scheme, every node's public keys are determined by information that uniquely identities them, such as IP address, email address, and/or MAC address rather than an arbitrary string.

4. ISMANET: Identity-Based Signcryption Secure Routing Protocol for MANET

The inheritance feature of ad-hoc network poses opportunities for attack ranging from passive eavesdropping to active impersonation, message replay, and message distortion. To cope with these attacks, we propose to employ features of network security in the routing protocols. Our goal is to provide a low overhead, fast computational time, and secure routing protocol in ad-hoc network. In order to achieve above goal, we use the identity-based signcryption scheme.

4.1 Attribute Definition

Table 1 presents the notation used in this paper.

Table 1 Attribute definitions.

Symbol	Definition
ID_X	Identifier of node X (MAC address)
Sig_X	Digital Signature of node X
H	One-way Hash Function H: $G_2 \rightarrow \{0,1\}_n$, H_1: $\{0,1\}^* \rightarrow G_1$, and H_2: $\{0,1\}^* \times G_2 \rightarrow F_q$.
$\hat{e}(P, Q)$	Bilinear map based on the Weil pairing
T	Authentication information
P, P_pub	Generator, Master key $\cdot$ P
k, r, V	Security parameter

Table 2 Algorithm for ISMANET.

```
<Sending RREQ Packet>
Sender node calculates security parameters and then
signs this message digest before sending a packet;

<Receive RREQ Packet>
Receiver node compares security parameters and checks
the signature;
if receiver node is the destination
     then it prepares to send RREP Packet;
else {
    the node makes any necessary modifications to the
          header and Receiver Node computes security
              parameters and signature;
     the node forwards packet to the next hop;
    }
```

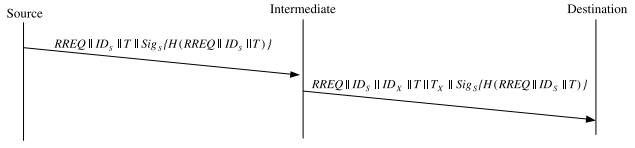


Fig. 1 Route request protocol.

4.2 Protocol Algorithm

Table 2 provides a detailed description of the proposed scheme.

4.3 Route Discovery

The route discovery process is abstracted as the exchange of two messages: a route request (RREQ) and a route reply (RREP).

4.3.1 Route Request

When a node wants to communicate with another node, it broadcasts an RREQ packet to its neighbors. A sender achieves the route discovery to establish a path to the destination. Figure 1 shows the request process.

A source node begins route instantiation to a destination node by broadcasting to its RREQ packet with the message for authentication. The RREQ packet contains the following fields <*source_addr*, *source_sequence_#*, *broadcast_id*, *dest_addr*, *dest_ sequence_#*, *hop_cnt*>. The functions of RREQ fields in this protocol are the same as those of RREQ fields of the general AODV.

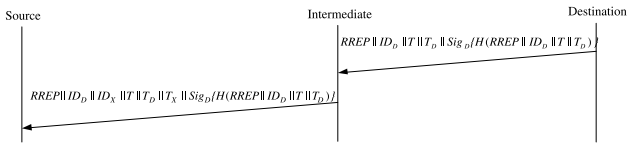


Fig. 2 Route reply protocol.

Using ID, the source node the computes public key $PK_S = H_1(ID_S)$ and the private key $SK_S = SK^* PK_S$ where SK^* is a system-wide master secret key. The key generation service in a distributed fashion requires an adversary to corrupt at least t nodes in order to obtain the system master secret key [1][14]. The node chooses a random number, x, and computes $k = \hat{e}(P, P_{pub})^x$ for the message's origin and both $r = H_2(k \parallel PK_s \parallel RREQ)$ and $V = xP_{pub} - rSK_S \in G_1$ for the authentication of nodes. The source sends routing request messages, $T = (r, V)$, and the created values, all of which are signed. The signature Sig is defined as follows: Sig=Signcrypt(*security parameters*, *private key*, *message*). Notice that signing does not involve any pairing calculations and thus it can be very quickly done even on low-end processors.

When an intermediate node $X_i (1 \leq i \leq n)$ receives the message, X_i first verifies the signature of source node, and then the node computes $\acute{k} = \hat{e}(P, V)\hat{e}(P_{pub}, PK_S)^r$ for the message's origin and checks $r = H_2(\acute{k} \parallel PK_S \parallel RREQ)$ for the validity of T received from the sender node. The $\acute{k}$ is verified by $\hat{e}(P, V)\hat{e}(P_{pub}, PK_S)^r = \hat{e}(P, P_{pub})^x$ which is computed by bilinearity of the map [3], [7]. The verification of signature is defined as follows: Valid=Unsigncrypt(*Sig*, *public key*, *security parameters*, *message*). *Valid* is a binary value that is set to 0 if the signature is invalid, and to 1 if the signature is valid. If the confirmation is successful, the source and intermediate node will trust each other and this process is finished successfully. Finally, the node broadcasts the message to the next nodes.

When the destination node receives the message, it checks the destination address. If the destination address is the same as its address, it verifies the signature and computes T and T_X. If the authentication is successful, the destination node is ready to reply a message. Otherwise, the packet is dropped.

4.3.2 Route Reply

The destination node generates an RREP packet, and sends the source node. Figure 2 shows the route reply process.

The destination node unicasts an RREP packet with a message for authentication back along the reverse path to the source node. The RREP packet contains the following fields <*source_addr*, *dest_addr*, *dest_sequence_#*, *hop_cnt*, *next_hop*, *lifetime*>. Also, the node adds T_D because the source node can trust the right reply to the message. The computation method of T_D in the route reply follows the similar way in RREQ. It computes $k = \hat{e}(P, P_{pub})^x$, and then

it computes $r = H_2(k \parallel PK_D \parallel RREP)$ and $V = xP_{pub} - rSK_D$ using the result of $k = \hat{e}(P, P_{pub})^x$.

A node sends a reply to inform its neighbor that it wishes to send a reply. The RREP message has a field that contains authentication information, T_X, for the neighbor. When the intermediate node receives the message, it verifies digital signature and computes the authentication information received from the sender node whether it is equal or not. If the digital signature and T_D are valid, the intermediate node can trust the message. The intermediate node receives the RREP, and then generates new authentication information and sends it to the node which sent the reply. If an authentication fails during the route request, the packet is dropped.

When the source node receives the RREP packet with a message for authentication, it verifies authentication information returned by the destination node as well as the destination node's signature. If the verification of the digital signature and the T value is successful, the secure route can be established over the channel. Since the replies are authenticated, these routes are valid and can be used for sending data packets.

4.4 Route Maintenance

If a path between source node S and destination node D is broken by link failure because either the destination or some intermediate nodes move during an active session, a node X which detects link failure generates an route error message (RERR) for its neighbor and sends the RERR message to source as follows:

Intermediate → Source

$< RERR \parallel ID_X \parallel ID_{X\_1} \parallel T \parallel T_X \parallel Sig_X\{H(RERR \parallel ID_X \parallel ID_{X\_1} \parallel T \parallel T_X)\} >$

Upon receiving notification of a link failure of node X_{-1}, nodes subsequently relay that message to their active neighbors. This message is forwarded along the path towards the source without modification. The break in the link is realized by using the MAC layer detection [6], [12]. This error message is sent whenever a node detects a break in the link with its neighbor. The nodes, which receive the RERR message, update their routing table. This process continues until all active nodes are notified.

To prevent unauthorized nodes from sending RERR, we require that an RERR be authenticated by the sender. Each node on the return path to the source forwards the RERR. Malicious nodes cannot generate RERR messages for other nodes because messages are signed and they cannot compute the authentication information. The computation method of in the route maintenance follows the similar way in route discovery. The number of route error packets sent is very small [6], [12]. Also, the RERR messages propagate to a few hops. They have negligible effect on the results.

Table 3 Basic statement.

Conjunction	Description
$P \mid\equiv X$	P believes X, or P would be entitled to believe X
$P \triangleleft X$	P sees X
$P \mid\sim X$	P once said X
$P \mid\Rightarrow X$	P has jurisdiction over X
$\sharp(X)$	The formula X is fresh
$P \overset{K}{\leftrightarrow}$	P and Q may use the shared key K to communicate
$\overset{K}{\mapsto} P$	P has K as a public key
$P \overset{X}{\Leftrightarrow} Q$	The formula X is a secret known only to P and Q, and possibly to principals trusted by them
$\{X\}_K$	This represents the formulas X encrypted under the key K
$\langle X\rangle_Y$	This represents X combined with the formula X

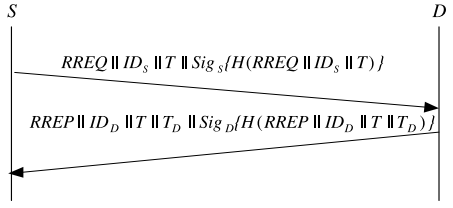


Fig. 3 Simplified protocol.

5. Correctness Proof of Protocol

The basic notation used in this section is provided here, as in [6], [13]. The symbols A, B, and S denote specific principals. The symbol P, Q, and R range over principals; X and Y range over statements; K ranges over encryption keys. Table 3 illustrates the basic statements.

We make the simplified protocol for verification such as Fig. 3.

The expressions of the idealized protocol for the proof are as follows:

$$M_1 : S \rightarrow D : \{T, H(RREQ, ID_S, T)\}_{K_S^{-1} \| K_S}$$
$$M_2 : D \rightarrow S : \{T, T_D, H(RREP, ID_D, T, T_D)\}_{K_S^{-1} \| K_D}$$

We have omitted cleartext communication simply like proof logic because it can be forged, and so its contribution to an authentication protocol is mostly one of providing hints as to what might be placed in encrypted messages. More detailed proof will be presented in Appendix.

6. Performance Evaluation

The goal of this section is to evaluate and emperically verify the effects of integration of the security scheme into ad-hoc network routing protocol and propose suitable security method to ad-hoc networks. In this section, we show the simulation results of the protocol.

6.1 Simulation Environment and Metrics

We have used the ns-2 simulator [10] for our evaluation. The

Table 4 General parameters used for all simulations.

Parameter	Value
Transmitter range	250 m
Bandwidth	2 Mb / s
Simulation time	900 s
Environment size	900 m × 300 m
Traffic type	CBR (Constant Bit Rate)
Packet rate	4 packets / s
Packet size	512 byte
Pause time	10, 50, 100, 200, 400, 800 s

original AODV protocol is used as a benchmark to study the performance evaluation of ISMANET. The RREQ and RERR packets are treated as broadcast packets in the MAC. RREP and data packets are all unicast packets with a specified neighbor as the MAC destination. Table 4 shows a summary of the simulation parameter.

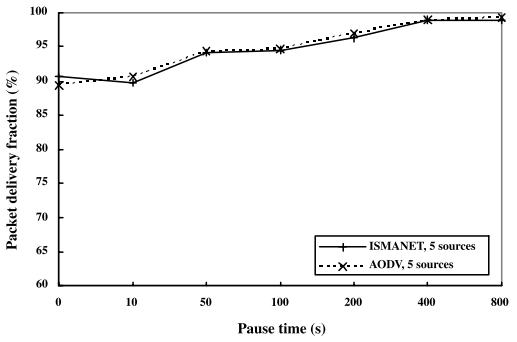
The radio model uses characteristics similar to a commercial radio interface, the 914 MHz Lucent's WaveLAN [4] DSSS radio interface. WaveLAN is modeled as shared-media radio with a nominal bit rate of 2 Mb/s and nominal radio range of 250 meters. In our experiments, 25 nodes move around in a rectangular area of 900 m × 300 m according to a mobility model i.e., the random waypoint model [8]. For the work related to energy-aware routing, we assume long-lived sessions. The session sources are CBR and generate UDP packets at 4 packets/sec with each packet being 512 bytes long in 900-second simulated time. The nodes are spread randomly over the network. Each node starts its journey from a random location to a random destination with randomly chosen speed. We vary the pause time, which affects the relative speeds of the mobiles.

The traffic and mobility models are the same as [16]. Three key performance metrics are evaluated in our experiments:

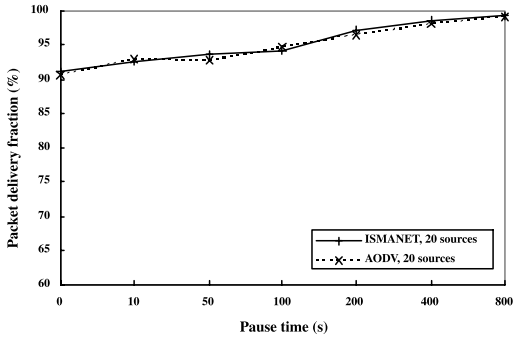
- Packet delivery fraction: The ratio of the data packets delivered to the destinations to those generated by the CBR sources; also, a related metric, received throughput (in kilobits per second) at the destination has been evaluated in some cases.
- Average end-to-end delay of data packets: This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer time.
- Normalized routing load: The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission.

6.2 Simulation Results

In this subsection, we mainly observe the effect when the routing authentication scheme using our identity-based signcryption scheme is applied on an ad-hoc network. We start the simulations in order to compare the original AODV routing protocol without any security requirements and the ISMANET routing protocol. The set of experiments uses differing numbers of sources with a moderate packet rate and varying pause times. We used 5 and 20 traffic sources and varied the pause time that means high pause time is low mobility and small pause time is high mobility. After each simulation was processed, trace files recording the traffic and node movement are generated. We then parsed those trace files in order to extract the information and statistics needed to measure each performance metric. We have done this study to illustrate that our scheme works for many security issues in the routing protocol, without causing any substantial degradation in the network performance.



(a) 5 sources

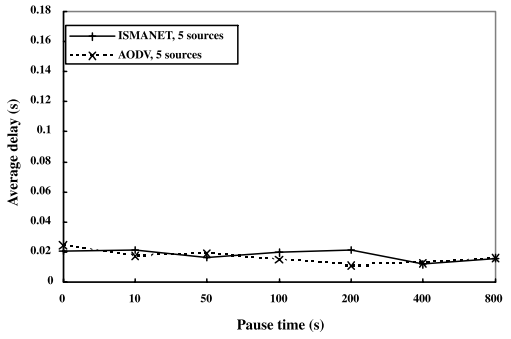


(b) 20 sources

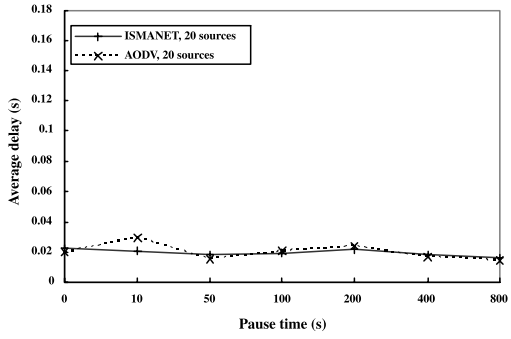
Fig. 4 Packet delivery fraction (%) for the 25-node model with various numbers of sources.

As the results shown in Fig. 4, our ISMANET protocol works well because the effect of throughput of the network is small around 2–10%. The packet delivery fractions for AODV and ISMANET are very similar with 5 and 20 sources. With 20 sources, however, has a better delivery fraction than AODV at higher pause times (Fig. 4(b)). However, if other realistic scenarios, for example, disaster scenarios, battlefield scenario, or very high-speed scenarios take this scheme, the effect of throughput of the network may reduce more than this.

The average data packet delays (as shown in Fig. 5) are fairly low both with authentication (ISMANET) and without authentication (AODV) extension. ISMANET and AODV have almost similar delays with 5 and 20 sources. There is a small increase with 5 sources (Fig. 5(a)) due to the exchange of packets during the authentication phase of security pro-

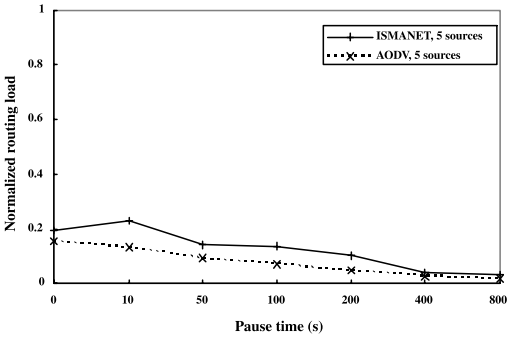


(a) 5 sources

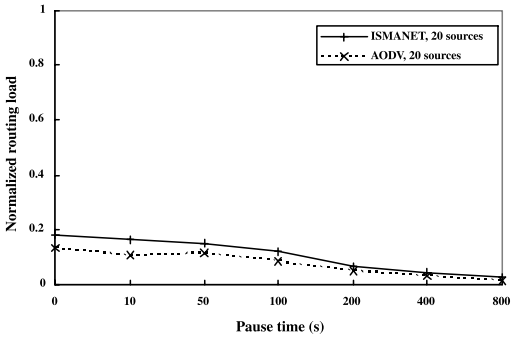


(b) 20 sources

Fig. 5 Average data packet delays for the 25-node model with various numbers of sources.



(a) 5 sources



(b) 20 sources

Fig. 6 Normalized routing loads for the 25-node model with various numbers of sources.

cess.

The number of routing packets increases when our scheme is incorporated. The increase in routing load is higher at lower pause time (Fig. 6). This is because at lower pause time, routes need to be found more frequently. The normalized routing loads of AODV and ISMANET are fairly stable with an increasing number of sources. A relatively stable normalized routing load is a desirable property for the scalability of the protocols, since this indicates that the actual routing load increases linearly with the number of sources.

7. Efficiency and Safety Analysis

Ad-hoc network has some distinct features such as the limited bandwidth and battery, and the frequent changes in topologies. To overcome these constraints, we use identity-based signcryption scheme based on pairings over elliptic curves [3], [7] for checking the generation and verification of the digital signature instead of RSA algorithm. The proposed protocol has some obvious advantages. First, unlike the traditional protocols, it needs no certificate, authentication of a public key, and public key directory because it uses identity-based cryptosystem. This identity-based scheme can eliminate the storage consumption and the certificate public key exchange dramatically when the network scalability is increased. Second, signcryption scheme used in this protocol can simultaneously fulfill both the functions of digital signature and encryption so it shows the dramatic reduction of computational cost and communication overhead than other schemes which fulfill these two functions independently. Third, the elliptic curve cryptography used in this protocol is relatively quick signature generation and key generation than other protocols based on RSA [9]. In this section, we analyze the performance of efficiency and safety.

7.1 Efficiency Analysis of Protocol

Across our experiments, we observe that ISMANET sends fewer routing protocol control messages (RREQs, RREPs, and RERRs) for the same number of flows and the same amount of application data.

7.1.1 Analysis 1: Calculating Overhead

ARAN [2] uses the RSA, and ISMANET and SRP [15] use the ECC public key cryptosystem for authenticating a node. However, Ariadne [17] and some other protocols use only the symmetric cryptography such as hash function and DES [5]. An elliptic curve $E(Z_P)$ with a point $P \in E(Z_P)$ whose order is 160 bit prime offers approximately the same level of security as DSA with 1024-bit modulus p and RSA with a 1024-bit modulus n. Thus, smaller parameters can be used in elliptic curve cryptosystems than with old discrete logarithm systems but with equivalent levels of security. The

advantages that can be gained from smaller parameters include speed (faster computations) and smaller keys. These advantages are especially important in environments where processing power, storage space, bandwidth, small hardware processor, and power consumption are constrained like the ad-hoc network. The communication overhead for each protocol is as follow:

$$CO = \sum_{i=1}^{x} (n \mid H \mid + n \mid E \mid + n \mid S \mid + n(packet \times 8))_i \qquad (1)$$

where CO is the communication overhead, n_i is the number of execution of ith node, $\mid E \mid$ is encryption, $\mid S \mid$ is signature, $\mid H \mid$ is hash function, and packet is RREQ, RREP, or RERR. We exclude the Aridne protocol in the comparison of computation because it is based on the different encryption scheme.

Total overhead is value of communication overhead and computation cost. Computation cost is 2.17 (ISMANET), 4.5 (ARAN), and 5.17 (SRP), respectably [22]. The total overhead for each protocol is as follow:

$$TO = \sum_{i=1}^{x} (CO \times ComputationCost)_i \qquad (2)$$

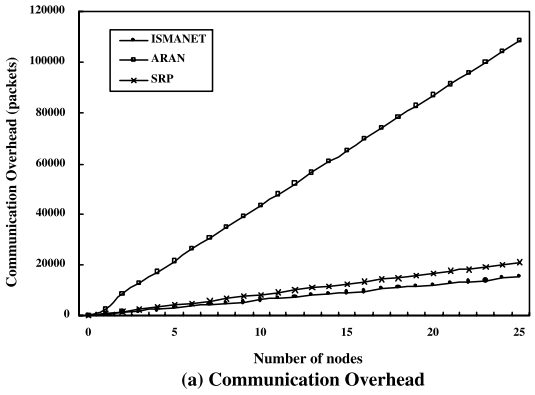
where TO is the total overhead. Figure 7 shows the simulation results which compare the previous protocol with the ISMANET in the calculating overhead. The communication overhead of ARAN is higher than our protocol and SRP because public key certificate and many sign and verify of message. The graphs show that the overhead of the ISMANET in terms of routing load is very low because computation cost of signcryption is very low than the other schemes.

7.1.2 Analysis 2: Computation Time

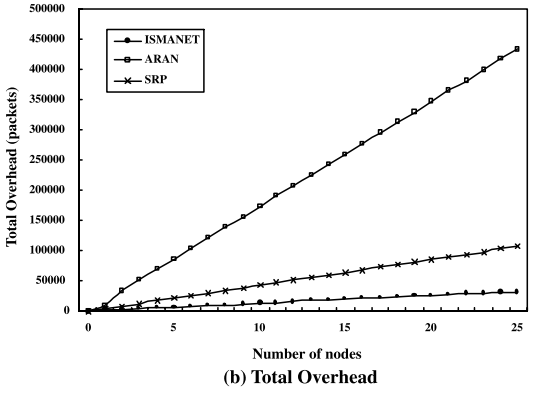
The signature time in RSA is 0.109 and the verification time is 0.037. However, in the proposed protocol, the signature time is only 0.006, and the verification time is just 0.012 [9]. What is more, it has the shorter key size than RSA because using the ECC. The time of computation in the whole network is as follow.

$$Time = nH + nE + n \mid p_a \mid + n \mid p_b \mid \qquad (3)$$

where $Time$ is the computation time in each node, E is the encryption time, $\mid p_a \mid$ is the generation time of signature, and $\mid p_b \mid$ is the verification time. This simulation excludes the broadcast time of network packets such as RREQ to describe the efficiency of cryptography. That is, this simulation shows only the time of cryptography. Table 5 shows the time of computation which compares the previous protocol with the proposed protocol. The computation time of each protocol is classified into two stages - ARAN stage 1 and ARAN stage 2 - and it is listed as follows. The ARAN stage 1 is for source to verify that the intended destination was reached and the ARAN stage 2 is optional stage that ensures shortest path.



(a) Communication Overhead



(b) Total Overhead

Fig. 7 Calculating overhead.

Table 5 Computation time.

Computation time	Scheme	ISMANET (160 bit)	ARAN 1024 bit	SRP 160 bit
ARAN Stage 1	Source	0.416 s	0.218 s	0.41 s
	Intermediate	0.422 s	0.292 s	0.416 s
ARAN Stage 2	Source	0.416 s	1.903 s	0.416 s
	Intermediate	0.422 s	1.977 s	0.416 s

Table 6 Comparison of ISMANET and other protocols.

Scheme	ISMANET	ARAN	SRP
Key distribution	Public key (Id-based signcryption)	Public key (RSA)	Public key (ECC)
Key management	Distributed	Centralized	Centralized
Intermediate node authentication	Yes	No	No
Certification	Not need	Need	Not need
Communication overhead	Low	High	Low
Computation cost	Low	High	High
Cost in Computation and Communication	≈Cost (signature)	Cost (signature) + Cost (encryption)	≈ Cost (encryption) + Cost (hash)

7.1.3 Analysis 3: Comparison of Secure Routing Protocols

Table 6 summarizes all the comparisons we have carried out in this paper, in terms of savings in computation cost and communication overhead.

7.2 Safety Analysis

Security is important and necessary to protect messages during their transmission and to guarantee that message transmissions are authentic. The proposed routing protocol can authenticate all of the nodes on routes with security parameter like k, T generated by each node based on identity-based signcryption scheme while ARAN and SRP cannot authenticate all nodes on routes. The safety of this protocol results in Bilinear Diffie-Hellman Assumption. We assume two cyclic groups, G_1 and G_2 which has a large prime order, q. P, an element of G_1, is selected randomly. aP, bP, cP are defined when a, b, c is selected randomly. We assume that it is difficult to compute $\hat{e}(P, P_{pub})^{abc}$. The safety of identity based scheme and signcryption scheme is verified by [3], [7].

Each node can verify the ID and the public key of each node so malicious nodes cannot hide their identity. In addition, the malicious nodes cannot fabricate the messages because the message is singed by the source and they do not know the secret key of the signature. Also, an attacker cannot obtain the master secret key unless it breaks into at least $t - 1$ members and obtains correct shares of the master private key. As a result of this, the proposed protocol is safe from fabrication attacks. Similarly, it can provide robustness from modification. When they modify the RREQ, RREP, or RERR packets, they cannot generate the correct hash value because they do not know the security parameter. In this protocol, ID is a MAC address. When each node transmits messages, it adds RREQ, RREP, or RERR packets to its IP address and MAC address as ID. Hence, this protocol can provide safety from snooping attacks because the IP address and the MAC address of a malicious node is not equal to values in the MAC address table.

8. Conclusions and Future Work

In this paper, we have focused on the efficiency of computation for the security of routing protocols in the ad-hoc network environment. We simulated our scheme using the ns-2 simulator. The results of our implementation show that the overheads caused by our scheme is marginal, while is ascertained that the system withstands attacks from numerous types of security breakers. This protocol has an advantage that it does not need to authenticate the public key because it uses the identity-based scheme. It can reduce network resources and communication overheads than the conventional secure routing because of the features of identity-based signcryption with pairing on elliptic curve. However, our protocol is operated in managed-open environment so that it can just guarantee the security in small local areas. We will study a securer protocol to guarantee the robustness in the wide area and not only to protect external attacks but also to detect the serious attacks from the compromised nodes and selfishness nodes.

References

[1] A. Khalili, J. Katz, and W.A. Arbaugh, "Toward secure key distribution in truly ad-hoc networs," SAINT-w'03, 2003.
[2] B. Dahill, B.N. Levine, E. Royer, and C. Shields, "ARAN: A secure routing protocol for ad hoc networks," UMass Tech Report 02-21, 2002.
[3] B. Libert and J-J. Quisquater, "New identity based signcryption schemes from parings," full version, available at http://eprint.iacr.org/2003/023/
[4] B. Tuch, "Development of WaveLAN, and ISM band wireless LAN," AT&T Tech. J., vol.72, no.4, pp.27–33, July/Aug. 1993.
[5] B. Schneier, Applied Cryptography, Second edition, Essential reference for cryptographic engineers by the foremost pundit in the field, Wiley, 1996.
[6] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999.
[7] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," Advances in Cryptology-Crypto'01, LNCS 2193, Springer, 2001.
[8] J. Broch, D.A. Maltz, D.B. Johnson, Y.-C. Hu, and J. Jetcheva, "A performance comparison of multihop wireless ad hoc network routing protocols," Proc. IEEE/ACM MOBICOM'98, pp.85–97, Oct. 1998.
[9] J. Lopez and R. Dahab, "Performance of elliptic curve cryptosystems," Technical Report IC-00-08, 2000., http://www.dcc.unicamp.br/ic-main/publications-e.html
[10] K. Fall and K. Varadhan, eds., "ns Notes and Documentation," 2003, available from http://www.isi.edu/nsnam/ns/
[11] L. Zhou and Z.J. Hass, "Securing ad hoc networks," IEEE Network Magazine, vol.13, no.6, pp.24–30, Nov. 1999.
[12] L. Venkatraman and D.P. Agrawal, "Strategies for enhancing routing security in protocols for mobile ad hoc networks," J. Parallel Distrib. Comput., vol.63, no.2, pp.214–227, Feb. 2003.
[13] M. Burrows, M. Abadi, and R. Needham, A Logic of Authentication, Digital System Research Center, Technical Report 39, Feb. 1990.
[14] M. Ilyas, The Handbook of Ad-Hoc Wireless Networks, CRC PRESS, 2002.
[15] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," Proc. CNDS 2002, San Antonio, TX, Jan. 2002.
[16] S.R. Das, C.E. Perkins, and E.M. Royer, "Performance comparison of two on-demand routing protocols for ad hoc networks," INFOCOM'2000, 2000.
[17] Y.C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Proc. MOBICOM 2002, 2002.
[18] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)," Advances in Cryptology-Crypto'97, LNCS 1294, pp.165–179, Springer, 1997.

Appendix

The appendix presents a formal analysis of the ISMANET and verifies the proof correctness of our protocol. The analysis follows the methodology of [16] which explained in the section 5.

First, we state the assumed initial beliefs of the player:

$$S \mid\equiv \overset{K_S^{-1}\|K_S}{\mapsto} S \qquad D \mid\equiv \overset{K_D^{-1}\|K_D}{\mapsto} D$$

$$S \mid\equiv \overset{K_D^{-1}\|K_D}{\mapsto} D \qquad D \mid\equiv \overset{D_S^{-1}\|K_D}{\mapsto} S$$

$$S \mid\equiv \sharp(T) \qquad D \mid\equiv \sharp(T)$$

The proof is as follows: From M1, via the message-meaning rules, we obtain:

$$D \lhd (RREQ, ID_S, T)$$
$$D \mid\equiv S \mid\sim H(RREQ, ID_S, T)$$

With upper equations, we postulate:

$$\frac{D \mid\equiv S \mid\sim H(RREQ, ID_S, T), D \lhd (RREQ, ID_S, T)}{D \mid\equiv S \mid\sim (RREQ, ID_S, T)}$$

Using T jurisdiction rule, we also derive:

$$D \mid\equiv S \mid\equiv T$$

That is,

$$\frac{D \mid\equiv S \mid\Rightarrow T, D \mid\equiv S \mid\equiv T}{D \mid\equiv T}$$

Thus,

$$D \mid\equiv S \overset{T}{\Leftrightarrow} D$$

M2 produces:

$$S \lhd (RREP, ID_D, T, T_D)$$
$$S \mid\equiv D \mid\sim H(RREP, ID_D, T, T_D)$$

Similarly to M1,

$$\frac{S \mid\equiv D \mid\sim H(RREP, ID_D, T, T_D), S \lhd (RREP, ID_D, T, T_D)}{S \mid\equiv S \mid\sim (RREP, ID_D, T, T_D)}$$

Using T and TD for jurisdiction rule, we obtain:

$$S \mid\equiv D \mid\equiv T, T_D$$

Also, we deduce:

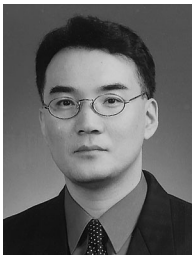
$$\frac{S \mid\equiv D \mid\Rightarrow T, T_D, S \mid\equiv T, T_D}{S \mid\equiv T, T_D}$$

Finally,

$$S \mid\equiv D \overset{T,T_D}{\Longleftrightarrow} S$$

Accordingly, S trusts *RREP* message from D and then D can construct the source-route of the reply packet. There is only one reply route defined in the source-route because we assume that there is no compromised node. In addition, the reply route is the same as the discovery route alone which *RREQ* has transmitted so that it is supposed that the *RREP* message has not been modified. Thus, the destination of *RREP*, S, can believe the connectivity information. The proof of *RERR* is similar to that of upper protocol.

Bok-Nyong Park received the B.S. degree in Computer Engineering from Hansung University, Seoul, Korea, in 2001. He received M.S. in Computer Science and Engineering from Korea University, Seoul, Korea, in 2003. He is currently a Ph.D. student in the Department of Computer Science and Engineering at the Korea University, Seoul, Korea His research interests include DRM, network security, Ad-Hoc networks, and Ubiquitous/Pervasive Computing.



Wonjun Lee is Assistant Professor in the Department of Computer Science and Engineering at Korea University, Seoul, Korea. Dr. Lee has held the faculty position at the University of Missouri - Kansas City, USA. He received the B.S. and M.S. degrees in computer engineering from Seoul National University, Seoul, Korea in 1989 and 1991, respectively. He also received the M.S. in computer science from the University of Maryland, College Park, USA in 1996 and the Ph.D. in computer science and engineering from the University of Minnesota, Minneapolis, USA, in 1999. His research interests include mobile wireless communications, wireless sensor networking, ubiquitous networking middleware, and Internet architecture technology. He has authored or co-authored over 45 papers in refereed international journals and conferences, and authored two invited book chapters. Since 2000, Dr. Lee has served on the program committees of more than 30 international conferences. He has also served AINA-2004 and AINA-2005 as PC Area Chair. He is a member of IEEE.