Efficient Authentication Scheme for Routing in Mobile Ad Hoc Networks

Shidi Xu, Yi Mu, and Willy Susilo

School of Information Technology and Computer Science,
University of Wollongong, Australia
{sdx86, wsusilo, ymu}@uow.edu.au

Abstract. The security deployment in mobile ad hoc networks is frequently hampered by resource constraints. The current routing systems of mobile ad hoc networks deploy very weak security techniques in order to copy with the computational overhead and bandwidth consumption. In this paper, we present an ID-based online/offline signature scheme which provides a full scale of security with sound performance. We show that our scheme is secure against existential forgery under adaptive chosen message attacks.

Keywords: Authentication, Digital Signature, MANET, Routing, AODV.

1 Introduction

The security technology deployed in the existing mobile ad hoc networks (MANET) is very weak, since the resource constraint makes complex security computations infeasible. Several well-known MANET routing protocols such as DSR [7] and AODV [8] were designed without a security consideration. Consequently, MANET routing systems face a number of security threats, from basic spoofing attacks to more complex rushing attacks. How to provide full-scale security to MANET with a low computational overhead and bandwidth consumption becomes an open problem to security researchers.

The security deployment to MANET is stunted by cryptographic techniques themselves, since they are expensive to configure and perform. In a MANET, each node is highly mobile,and hence it requires the routing operations to be accomplished within their lifetime; otherwise the routing information will not be able to represent the current topology condition. In addition to computational overhead, MANET also has problems in key distribution. This is particularly important in routing, because in a routing system, mobile nodes are not aware of other nodes that are out of their radio signal broadcasting diameter. This is usually roughly handled by a pre-key distribution phase. However, in an ad hoc network, which is formed impromptu, the authentication between nodes is performed in a cursory manner.

Our Contribution. In this paper, we introduce a novel authentication scheme to tackle the problem of computational overheads in MANET. We devise a novel

T. Enokido et al. (Eds.): EUC Workshops 2005, LNCS 3823, pp. 854–863, 2005.

digital signature scheme that is especially feasible for authentication in MANET. In our scheme, a signing operation is split into two phases: offline phase and online phase. The major computational overhead is shifted to the offline phase, whereas the online phase requires only a very low computation overhead to achieve a full scale of authentication. Moreover, the public key distribution problem is solved by using node's identity such as IP or MAC address as its public key. We will also describe how this signature can be used for securing an AODV routing system.

Organization of the paper. The rest of the paper is organized as follow. In section 2, we introduce several secure routing protocols, the concept of online/offline signature, and review previous works. In section 3, we give some preliminaries of bilinear pairings and definitions. In section 4, we define the generic scheme and attack model. In section 5, we present our scheme and analyze its security. In section 6, we describe how to apply our scheme to the AODV routing system. In the last section, we conclude the paper.

2 Previous Work

2.1 Secure Routing Protocol

To protect MANET routing systems against various attacks, a sound authentication scheme must be deployed. There have been several schemes in the literature. Each of them uses a different method in providing sender authentication and message integrity.

Ariadne, proposed by Hu, Perrig and Johnson [6], is a secure on-demand routing protocol based on DSR. The security of Ariadne generally relies only on highly efficient symmetric-key cryptography. It assumes a pre-deployed secret shared between the sending node and targeting node. The authentication between intermediate nodes is done using the TESLA authentication protocol. During the transmission of route requests, each intermediate node appends a MAC generated using TESLA key. This MAC will be authenticated when a route reply is transmitted back to the originator. Since the TESLA authentication protocol is used, each node must be loosely time synchronized to decide the validity of TESLA keys, which becomes the major drawback of Ariadne.

SAODV [10] is a security extension of the AODV routing protocol. Since the routing operation in AODV is very simple, its security requirement can be easily satisfied. SAODV uses conventional digital signatures to protect routing messages. However, it neither deploys the public key certificate nor assumes pre-shared secret between nodes. Each sending node signs its own public key along with routing messages. The key distribution problem is loosely solved with some compromise of security.

2.2 Online/Offline Signature

The online/offline digital signature scheme was firstly introduced by Even, Goldreich and Micali [4]. The basic concept of their scheme is splitting the signature

generation algorithm into two phases: offline phase and online phase. To achieve efficient performance when a message is coming to be signed, they utilize an offline phase to handle the most costly computation. When a message is ready, the online phase can be performed extremely efficient to generate the required signature. On drawback of their scheme is that the size of public key and resulting signature is likewise very large since one-time signature is used.

Zhang, Mu and Susilo [11] proposed the first online/offline signcryption scheme from bilinear pairings. The online signing phase is also very efficient in their scheme, which requires approximately one hash. The size of the resulting signature is reduced to $\log_2 p + \log_2 \rho + 160$, where p is the order of cyclic additive group and ρ is the safe length of that group,where the underlying cryptographic assumption still holds. Although this scheme has its merit, it is out of the scope of our aim since we consider the efficient authentication only.

3 Bilinear Pairings

Let $\mathbb{G}_1$ be a cyclic additive group generated by P, with a prime order q, and $\mathbb{G}_2$ be a cyclic multiplicative group with the same prime order p. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a map with with the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1, a, b \in \mathbb{Z}_q^*$;
2. Non-degeneracy: There exists $P, Q \in \mathbb{G}_1$ such that $e(P, Q) \neq 1$;
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in \mathbb{G}_1$;

The Non-degeneracy implies that when P is the generator of $\mathbb{G}_1$, $e(P, P)$ is the generator of $\mathbb{G}_2$. We call such bilinear map as an admissible bilinear pairing. Problems considered in the additive group $\mathbb{G}_1$ are:

- **Decisional Diffie-Hellman Problem (DDHP):** For $a, b, c \in \mathbb{Z}_q^*$, given P, aP, bP, cP decide whether $c \equiv ab \mod q$.
- **Computational Diffie-Hellman Problem (CDHP):** For $a, b \in \mathbb{Z}_q^*$, given P, aP, bP compute abP.

In bilinear pairings, Decision Diffie-Hellman problem (DDHP) is easy and Computational Diffie-Hellman problem (CDHP) is still hard. That is, for $a, b \in \mathbb{Z}_q^*$, given P, aP, bP, computing abP is infeasible.

Definition 1. *A group $\mathbb{G}$ is a gap Diffie-Hellman(GDH) if there exists a polynomial time probabilistic algorithm to compute the decisional Diffie-Hellman problem but exists no such algorithm to solve the computational Diffie-Hellman problem in $\mathbb{G}$.*

Above system parameters can be obtain through running the **GDH Parameter Generator** [3] $\mathcal{IG}$ which takes a security parameter $k \in \mathbb{Z}^+$ as input, runs in polynomial time in k, and outputs a prime number q, the description of two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, and the description of an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$.

Definition 2. *The advantage of an algorithm $\mathcal{A}$ in solving CDHP in group $\mathbb{G}$ is*

$$\mathsf{Adv}_{\mathcal{A}}^{CDH} = \Pr[\mathcal{A}(P, aP, bP) = abP : a, b \overset{R}{\leftarrow} \mathbb{Z}_q^*]$$

where the probability is over the choice of a and b, and the coin tosses of $\mathcal{A}$. We say that an algorithm $\mathcal{A}(t, \epsilon)$-breaks CDHP in $\mathbb{G}$ if $\mathcal{A}$ runs in time at most t, and $\mathsf{Adv}_{\mathcal{A}}^{CDH} > \epsilon$.

4 The Model

In this section we formalize the general online/offline digital signature paradigm. This paradigm is extended to elicit our ID-based scheme.

4.1 Generic Scheme

Online/offline digital signature scheme $\mathcal{DS}$ is comprised of four polynomial time algorithms: KeyGen, OffSign, OnSign, and Verify, called *key generation algorithm*, *offline signing algorithm*, *online signing algorith*, and *verification algorithm*, respectively. The first three algorithms are probabilistic.

KeyGen. On input 1^k, the algorithm produces a pair of matching public and secret keys (pk, sk).
OffSign. On input (sk, r), where r a signing parameter, the algorithm returns an offline signature S.
OnSign. On input (S, m), where S is the offline signature and m is the message, the algorithm returns an online signature σ.
Verify. On input (pk, m, S, σ), the algorithm returns 1 (*accept*) or 0 (*reject*).

The security for signature schemes was defined by Golwasser, Malia and Rivest [5] as secure against existential forgery under adaptive chosen message attacks (EF-CMA). We extend this notion to online/offline signature schemes as follow:

Definition 3. ***(Security)*** *[5] The online/offline signature scheme*
$\mathcal{S} =< KeyGen, OffSign, OnSign, Verify >$
is existential unforgeable under adaptive chosen message attacks if it is infeasible for a forger to produce a valid message-signature pair after obtaining polynomially many signatures on a message of its choice from the signer.
Formally, for every probabilistic polynomial forger $\mathcal{A}$ such that:

$$\mathsf{Adv}(\mathcal{A}) = \Pr\left[\begin{array}{l}(pk, sk) \leftarrow \mathsf{KeyGen}(1^k);\\ for\ i = 1, 2, ..., k, r;\\ m_i \leftarrow \mathcal{A}(pk, m_1, S_1, \sigma_1, ..., m_{i-1}, S_{i-1}, \sigma_k);\\ S_i \leftarrow \mathsf{OffSign}(sk, r),\ \sigma_i \leftarrow \mathsf{OnSign}(S_i, m);\\ (m, S, \sigma) \leftarrow \mathcal{A}(pk, m_1, S_1, \sigma_1, ..., m_k, S_k, \sigma_k);\\ m \neq m_1, ..., m_k\ and\ \mathsf{Verify}(pk, m, S, \sigma) = \text{accept};\end{array}\right] \leq \epsilon$$

4.2 Attack Model

The formal attack model for ID-based signature scheme was firstly generalized by Cha and Cheon in [2], which is called *existential forgery under adaptive chosen message and ID attack*(EF-IOS-CMA).

We can define our game between an attacker $\mathcal{A}$ and a challenger $\mathcal{C}$ as follow:

1. $\mathcal{C}$ runs Setup to obtain the system parameters which are given to $\mathcal{A}$.
2. $\mathcal{A}$ runs message hash query, ID extraction query, online and offline signing query to obtain necessary information.
3. $\mathcal{A}$ finally outputs (ID, m, S, σ), where ID is an identity, m is a message, S is offline signature, and σ is online signature, such that ID and (ID, m) are not in the inputs to extraction query and signing query. $\mathcal{A}$ wins the game if (ID, m, S, σ) is valid.

Definition 4. *The success probability of winning the above game is defined by* $\mathsf{Succ}_{\mathcal{A}}^{EF-IOS-CMA}(\ell)$. *An online/offline signature scheme is secure if the success probability of the above attack is negligible. In other words,*

$$\mathsf{Succ}_{\mathcal{A}}^{EF-IOS-CMA}(\ell) \leq \epsilon.$$

5 Our Scheme

Based on the general scheme, our ID-based online/offline scheme consists five algorithms: Setup, Extract, OffSign, OnSign, Verify.

Setup. Given $\mathbb{G}_1$ and its generator P, pick a random $s \in \mathbb{Z}_q^*$, and set $P_{pub} = sP$. Choose a cryptographic hash function $H_0 : \{0,1\}^* \to \mathbb{G}_1$ and $H_1 : \{0,1\}^* \times \mathbb{G}_1 \to \mathbb{Z}_q^*$. The system parameters are (P, P_{pub}, H_0, H_1). The master key is s. H_0 and H_1 behave as random oracles [1].

Extract. Given an identity ID, the algorithm computes $D_{ID} = sH_0(ID)$ and output it as the private key related to ID corresponding to $Q_{ID} = H_0(ID)$.

OffSign. Given a secret key D_{ID}, pick a random number $r \in \mathbb{Z}_q^*$ and a random secret number $x \in \mathbb{Z}_q^*$, output the offline signature pair (S, R), where $S = \frac{1}{r}D_{ID}$, $R = xP$.

OnSign. Given a message m and offline signature S, compute the online signature as $\sigma = H_1(m, R)x + r$. The resulting signature is a triple (s, σ, R).

Verify. Given a signature tuple (S, σ, R) of a message m for an identity ID, check whether $(P_{pub}, \sigma P - H_1(m, R)R, S, Q_{ID})$ is a valid Diffie-Hellman tuple.

5.1 Analysis

In this section, we will discuss the correctness and efficiency of our scheme.

Correctness: The correctness can be easily proved as follow:

$$\begin{aligned} e(\sigma P - H_1(m,R)R, S) &= e(xH_1(m,R)P + rP - H_1(m,R)R, \quad \frac{1}{r}D_{ID}) \\ &= e(H_1(m,R)xP + rP - H_1(m,R)xP, \quad \frac{1}{r}D_{ID}) \\ &= e(rP, \quad \frac{1}{r}sQ_{ID}) \\ &= e(P_{pub}, \quad Q_{ID}) \end{aligned}$$

Signature Size: The resulting signature is the tripe (S, σ, R). We assume the safe length of GDH group $\mathbb{G}_1$ is ρ, the size of each element in a signature tuple is $\log_2 \rho$, $\log_2 q$, and $\log_2 \rho$. Therefore, the total length is $2\log_2 \rho + \log_2 q$. We believe this size is irreducible since the first two elements are required in all the standard ID-based signature scheme.

Performance: Obviously, the online phase of our scheme is very efficient, which only requires one hash, one multiplication, and one addition. The computational workload is passed to the offline phase. The signature verification is done through two pairing operations, which is the most expensive part in our scheme. However, since $e(P_{pub}, Q_{ID})$ is a constant, it only needs to be computed once.

5.2 Security Proof

To prove our scheme is secure against *adaptive chosen message and ID attack*, the problem is firstly reduced to a *given* ID attack. Specifically, we intend to view the scheme as an ordinary ID-based signature scheme which outputs two signatures. Since the online signing phase does not using ID information, it can be viewed as an sub-phase of ID-based offline signing phase.

Specifically, we intend to view the scheme as an ordinary ID-based signature scheme which output two signatures. Since the online signing phase does not using ID information, it is viewed as an sub-phase of ID-based offline signing phase.

Lemma 1. *Let $\mathcal{A}_0$ be an algorithm for an adaptive chosen message and ID attack to our scheme with running time t_0 and advantage ϵ_0, then there is an algorithm $\mathcal{A}_1$ for an adaptive chosen message and given ID attack which has running time $t_1 \leq t_0$ and advantage $\epsilon_1 \leq \epsilon_0(1 - \frac{1}{q})/q_{H_0}$, where q_{H_0} is the maximum number of queries to ID hash oracle H_2 asked by $\mathcal{A}_0$.*

Proof. We assume that the number of queries to message hash oracle, extraction oracle and online signing oracle are q_{H_1}, q_E, and q_S. Algorithm $\mathcal{A}_1$ is performed as follow:

1. Randomly choose $l \in \{1, ..., q_{H_0}\}$. Let ID_i denote the input of i^{th} q_{H_0} query asked by $\mathcal{A}_0$. Set ID_i' be ID^* if $i = l$, and ID_i otherwise. Define $H_0'(ID_i)$, $\mathsf{Extract}'(ID_i)$, $\mathsf{Sign}'(ID_i, m)$ to be $H_0(ID_i')$, $\mathsf{Extract}(ID_i')$, $\mathsf{Sign}(ID_i', m)$. Notice that the Sign includes $\mathsf{OffSign}$ and OnSign. However, only the offline signing part is considered in an ID attack, since the online signing part does not use any ID information.

2. Run $\mathcal{A}_0$ with the given system parameters. $\mathcal{A}_1$ responds to $\mathcal{A}_0$'s queries to H_0, H_1, Extract, and Sign by evaluating H_0', H_1, Extract', and Sign', respectively. Let the output of $\mathcal{A}_0$ be (ID_{out}, m, S, σ).
3. If $ID_{out} = ID^*$ and (ID_{out}, m, S, σ) is valid, the output (ID^*, m, S, σ). Otherwise output fail.
   Since the probability distributions provided by H_0', Extract', and Sign' are indistinguishable from those produced by H_0, Extract, and Sign, $\mathcal{A}_0$ learns nothing from query result. Besides, the probability that $\mathcal{A}_0$ produces a valid message signature pair (ID, m, S, σ) without any query of $H_0'(ID)$ is greater than $(1 - \frac{1}{q})$. Hence, we can say $\mathcal{A}_0$ wins the game with advantage $\geq \epsilon(1 - \frac{1}{q})/q_{H_0}$, where ϵ is an upper bound of success. □

Lemma 2. *If there is an algorithm $\mathcal{A}_1$ for an adaptive chosen message and given ID attack to our scheme which queries H_1, H_2, Sign and Extract at most q_{H_1}, q_{H_2}, q_S and q_E times respectively, and has running time t_1 and advantage $\epsilon_1 \geq 10(q_S+1)(q_S+q_{H_1})/q$, then CDHP can be solved with probability $\epsilon_2 \geq 1/9$ within running time $t_2 \leq 23 q_{H_1} t_1/\epsilon_1$.*

Proof. We assume that for any ID, $\mathcal{A}_1$ queries $H_0(ID)$ and Extract at most once. We have an algorithm $\mathcal{A}_1$, through interacting with a signing simulator $\mathcal{B}$, computes abP for a randomly given instance (P, aP, bP) where P is a generator of G.

1. Fix an identity ID and put $P_{pub} = aP$. Randomly choose $\alpha_i \in \mathbb{Z}_q^*$ *for* $i = 1, ..., q_E$ and $\beta_j, x_j \in \mathbb{Z}_q^*$ *for* $j = 1, ..., q_S$. Let ID_i *and* ID_{i_k} denote the input of the i^{th} H_0 query and the k^{th} Extract query. We define:

$$H_0''(ID) = \begin{cases} bP & \text{if } ID_i = ID^*, \\ \alpha_j P & \text{otherwise;} \end{cases}$$

$$\mathsf{Extract}''(ID_{i_k}) = \alpha_{i_k}(bP);$$

$$\mathsf{OffSign}''(m_j, x_j,) = (m_j, h_j, \sigma_j), \ \textit{where } h_j = H_1(m, R_j), \ \sigma_j = h_j x_j + \frac{a}{\beta};$$

$$\mathsf{OnSign}''(ID_{i_j}) = (ID_{i_j}, R_j, S_j), \ \textit{where } R_j = x_j P.$$

   The resulting signature is $(ID_j, m_j, R_j, S_j, \sigma_j)$. We observed that $(bP, \sigma P - Rh, S, aP)$ is valid Diffie-Hellman tuple since:

$$\begin{aligned} e((hx + \frac{a}{\beta})P - hR, S) &= e(hxP - \frac{a}{\beta}P - hxP, \beta bP) \\ &= e(\frac{a}{\beta}P, \beta bP) \\ &= e(aP, bP) \end{aligned}$$

2. We apply the oracle replay attack invented by Pointcheval and Stern in [9].
   (a) $\mathcal{A}_1$ firstly asks q_{H_1} distinct queries to the random oracle f, obtaining $\rho_1, ..., \rho_{q_{H_1}}$ answers respectively. Assume there is a simulator $\mathcal{B}$ which simulates the activity of signer without the knowledge of secret key. For

each query of message m_j it output a series of signature message pairs in the form of $(ID_j, m_j, R_j, h_j, S_j, \sigma_j)$. Then algorithm $\mathcal{A}_1$ assumes that $f(m_j, R_j) = h_j$ and stores it.

(b) If following collisions appear:
- A (m_j, R_j) pair produced by $\mathcal{B}$ also appears in the list of questions to random oracle asked by $\mathcal{A}_1$;
- $\mathcal{B}$ produces two (m_j, R_j) pairs which are exactly the same;

$\mathcal{A}_1$ simply outputs fail and aborts. If no collision appeared, $\mathcal{A}_1$ outputs a valid message signature pair, which is expected to be valid for the fixed ID.

(c) By replaying $\mathcal{B}$ with the same messages but different choice of H_1, we can obtain two valid signatures (ID, m, R, h, S, σ) and $(ID, m, R, h', S, \sigma')$, where $h \neq h'$. Notice that offline signatures are supposed to be the same since it is closely related to the value of r.

(d) If both outputs are valid, compute $x = \frac{\sigma - \sigma'}{h - h'}$.

3. Since $(Q_{ID_j}, \sigma_j P - R_j h_j, S_j, P_{pub})$ is valid Diffie-Hellman tuple, we can compute α through $\beta = \frac{a}{\sigma - h_j x_j}$. Apply β_j to S_j, we have

$$S = \frac{a}{\sigma - h_j x_j}(bP)$$
$$S = \frac{abP}{\sigma - h_j x_j}$$
$$abP = S(\sigma - h_j x_j)$$

□

Combining Lemma 1 and 2, we have the following theorems.

Theorem 1. *If there is an algorithm $\mathcal{A}_0$ for an adaptive chosen message and ID attack to our scheme which queries H_0, H_1, Sign and Extract at most q_{H_0}, q_{H_1}, q_S and q_E times respectively, and has running time t_1 and advantage $\epsilon_0 \geq 10(q_S+1)(q_S+q_{H_1})q_{H_0}/(q-1)$, then CDHP can be solved with probability $\geq 1/9$ within running time $\leq \frac{23 q_{H_0} q_{H_1} t_0}{\epsilon_0(1-\frac{1}{q})}$.*

Using another variant of the forking lemma [9], we have the following result:

Theorem 2. *If there is an algorithm $\mathcal{A}_1$ for an adaptive chosen message and given ID attack to our scheme which queries H_0, H_1, Sign and Extract at most q_{H_0}, q_{H_1}, q_S and q_E times respectively, and has running time t_1 and advantage $\epsilon_1 \geq 10(q_S+1)(q_S+q_{H_1})/q$, then CDHP can be solved within expected time $\leq 120686 q_{H_1} t_1/\epsilon_1$.*

Theorem 3. *If there is an algorithm $\mathcal{A}_0$ for an adaptive chosen message and ID attack to our scheme which queries H_0, H_1, Sign and Extract at most q_{H_0}, q_{H_1}, q_S and q_E times respectively, and has running time t_1 and advantage $\epsilon_1 \geq 10(q_S+1)(q_S+q_{H_1})q_{H_0}/(q-1)$, then CDHP can be solved within expected time $\leq \frac{120686 q_{H_0} q_{H_1} t_0}{\epsilon_0(1-\frac{1}{q})}$.*

6 Application for AODV

We now describe how to apply our scheme to the AODV routing protocol, which is quite straightforward and its security can be significantly reinforced by merely using digital signature. We will briefly introduce the security requirement of AODV routing protocol and then describe how our scheme can be implemented over it.

6.1 AODV Security Requirement

AODV is a simple and efficient on-demand ad hoc routing protocol. Basically, it uses RREQ (route request), RREP (route reply) and RRER (route error) messages to accomplish route discovery and maintenance operations. It also utilizes sequence numbers to prevent routing loops. Routing decision making is based on sequence numbers and routes maintained in each node's routing table.

We require that each node must submit its identity to the key generation center before entering the network through a secure channel. The key generation center will generate a private key correspondent to node's ID, and send it to the node along with necessary system parameters. In an ad hoc environment, this phase should be performed offline.

After entering the network, each node starts to compute its offline signature. Since the offline signature is created over a random value, the node can randomly choose several values and compute the signatures respectively for each session. When a routing request is initiated, the node generates a routing packet (RREQ/RREP) according to AODV and generate the online signature for this packet. This phase is very efficient since signature generation only requires one hash. Then the sender node broadcasts the packet and signature to neighbors.

When a neighboring node receives this packet, it will verify this signature and broadcast to the next hop. To be efficient, the verification can be done offline. The receiving node should broadcasts the packet before verification. However, only if this packet passes the verification, will the receiving update its routing table entry according to the information carried in the packet.

By deploying our scheme, the efficiency of SAODV can be improved. This scheme can also be used in some other routing protocol such as DSR, which requires much more frequent signing operations. Using bilinear pairing would engender the major cost in our scheme, but the realization of ID-based authentication scheme can largely solve the diehard key distribution problem in MANET.

7 Conclusion

We proposed an ID-based online/offline signature scheme from bilinear pairings that is suitable for MANET. In our scheme, the resulting signature is a triplet. The online signature can be computed is very efficient, approximately one hash operation. The computation of the offline phase requires only one scalar multiplication under an additive group. The verification is done through pairings

but its performance can be enhanced after the first execution. We proved that our scheme is secure against existential forgery under adaptive chosen message attacks based on the random oracle model. The security of our scheme is based on CDHP. Our scheme is especially suitable for mobile ad hoc networks routing where signature enabled authentication is to be performed in an efficient manner. We also discussed the implementation issue over MANET routing protocols and presented an implementation method over AODV routing protocol.

References

1. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proceedings of the First Annual Conference on Computer and Communications Security*. ACM, November 1993.
2. J. Cha and J. Cheon. An id-based signature from gap-diffie-hellman groups. In *Proceedings of Public Key Cryptography - PKC 2003*, volume 2567, pages 1–24. Springer-Verlag, 2003.
3. D.Boneh, B. Lynn, and H. Shacham. Short signature fromt eht weil pairing. In *Proceedings of Asiacrypt '01, Lecture Notes in Computer Sciences*, volume 2248, pages 514–532. MANET working group, 2001.
4. S. Even, O. Goldreich, and S. Macali. On-line/off-line digital signatures. In *Proceedings of Advances in Cryptology: Crypto '89*. Springer, 1990.
5. S. Glodwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal of Computing*, 17:281–308, 1988.
6. Y. C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. In *Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (Mobicom 2002)*, 2002.
7. D. B. Johnson, D. A. Maltz, and Y. C. Hu. *The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)*, 2004.
8. C. E. Perkins, E. M. Royer, and S. R. Das. *Ad Hoc On-Demand Distance Vector (AODV) Routing*, 2003.
9. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *Journal of Cryptology*, 13:361–396, 2000.
10. M. G. Zapata. *Secure Ad hoc On-Demand Distance Vector (SAODV) Routing*, 2004.
11. F. Zhang, Y. Mu, and W. Susilo. Reducing security overhead for mobile networks. In *Proceedings of The 19th International Conference on Advanced Information Networking and Applications (AINA 2005)*, pages 398–403. IEEE Computer Society, 2005.