

A Certificateless Signature Scheme for Mobile Wireless Cyber-Physical Systems

Zhong Xu^{*†} Xue Liu[†]

[†] School of Computer Science
McGill University
Montreal, Quebec H3A 2A7, Canada
{zhongxu,xueliu,wshu}@cs.mcgill.ca

Guoqing Zhang^{*} Wenbo He[‡]

[‡] Dept. of Computer Science
University of Illinois at Urbana-Champaign
Urbana, IL, 61801, USA
wenbohe@uiuc.edu

Guanzhong Dai^{*} Weihuan Shu[†]

^{*} College of Automation
Northwestern Polytechnical University
Xi'an 710072, Shaanxi, P.R. China
gniqoug@mail.nwpu.edu.cn, daigz@nwpu.edu.cn

Abstract

Due to the unique characteristics of Cyber-Physical Systems (CPS) such as interaction with the physical world, many new research challenges arise. Many CPS applications will be implemented on computing devices using mobile ad hoc networks (MANETs). Before these systems can be used in multifarious environments, the security properties of these networks must be fully understood.

Recently, several secure signature schemes for MANETs have been proposed based on public key cryptography and identity-based cryptography. In order to solve some problems in these schemes, such as the costly and complex key management problem in traditional public key cryptography and the “key escrow” problem in identity-based cryptography, the notion of certificateless public key cryptography was introduced. In this paper, we propose an efficient certificateless signature scheme for mobile wireless cyber-physical systems (McCLS) based on the bilinear Diffie-Hellman assumption. Empirical studies are conducted using QualNet to evaluate the effectiveness and efficiency of McCLS scheme under two most common attacks, i.e. black hole attack and rushing attack. Results show that McCLS scheme is more efficient than existing solutions and is able to resist these two kinds of attacks.

1. Introduction

A salient feature of Cyber-Physical System (CPS) is that it integrates computing, monitoring, and communication capabilities, and constantly interacts with the physical envi-

ronment. As a result, CPS must be dependable, safe, secure and efficient [9].

Many emergent applications proposed for CPS will be implemented on networked environments where computing devices are connected through wireless links. For many applications, there may be no fixed infrastructure available, or for military applications, infrastructures may be destroyed. As a result, the network environment of many future CPS applications may be ad hoc and need self-configuration capability. Networks that support mobile wireless ad hoc architecture are typically called mobile ad hoc networks (MANETs). While MANETs provide a great flexibility for establishing communications, it also poses a lot of research challenges. One of the major challenges is how to maintain system security facing the lacking of infrastructure, and dynamic topology changes for MANETs.

To solve one of the major security problems of MANETs, there have been several signature schemes for these networks based on public key infrastructure (PKI) [18, 14] and identity-based public key cryptography (ID-PKC) [5, 16].

In a traditional PKI signature scheme, a centralized certificate authority must be provided to issue a digital certificate binding a user with its public key. The requirement of certificate authority inevitably leads to complex certificate management problems in practice.

ID-PKC was introduced by Shamir [11] to simplify the certificate management process. In an ID-PKC based scheme, a user's public key is derived directly from certain aspects of its identity (such as email address) which is assumed to be publicly known. Private keys are generated for users by a trusted third party – Private Key Generator (PKG). However, a new inherent problem is brought by this

approach, namely a “key escrow” problem since the private keys of users are known to the PKG. As a result, the PKG may impersonate any user of its choice, or decrypt messages.

In order to overcome the drawbacks of ID-PKC based schemes, Al-Riyami and Paterson [1] proposed the first certificateless public key cryptography (CL-PKC) scheme. In a certificateless signature (CLS) scheme, Key Generation Center (KGC) only supplies a user with a partial private key, which is related to the user’s identity. The user generates the remaining part of the private key and its corresponding public key. The KGC does not know the user’s private key since the user generates the private key by itself, thereby solving the “key escrow” problem in ID-PKC based schemes.

However, CLS schemes are usually computationally intensive, hence they are not readily applicable to practical applications. In this paper, we present McCLS scheme, a new CLS scheme for mobile wireless cyber-physical systems. Compared with existing CLS schemes, McCLS scheme requires less computation overhead because it only requires one pairing operation in the verification phase, and none in the signature phase. We also provide a detailed security proof for McCLS scheme based on the the bilinear Diffie-Hellman assumption in the random oracle model. We compare the performance of McCLS scheme with several other schemes based on QualNet simulation [10] and show that McCLS scheme is more efficient in terms of computation overhead and it can resist against *black hole attack* [8] and *rushing attack* [6].

The remainder of the paper is organized as follows. Section 2 provides a brief description on the related work. Section 3 introduces the preliminaries and background on the security model. McCLS scheme is proposed in Section 4. In Section 5, the security analysis of McCLS scheme is presented in detail. Section 6 evaluates the performance of McCLS scheme under the black hole attack and the rushing attack. Finally, we conclude this paper in Section 7.

2. Related Work

CPS integrates the communication and computation with the physical process. Since CPS constantly interact with the physical environment, they must be dependable, safe, secure and efficient [9].

CPS is a new active research area. The position papers published in the NSF workshop on cyber-physical system [9] gives a good overview of different aspects of CPS research. Though security is an important research issue of CPS, little work has been done [2] so far for the security of CPS.

Since many emergent applications proposed for CPS will be implemented on MANETs, it is natural to ask the question if security schemes proposed for MANETs are prac-

tical for CPS. To overcome the problems such as the key management problem in public key cryptography and “key escrow” problem in identity-based cryptography schemes, recently, Al-Riyami and Paterson [1] proposed the first certificateless signature (CLS) scheme but with no security proof provided. Later, Huang et al. [7] found that this CLS scheme was insecure against a Type I forger attack. A modified CLS scheme was proposed with security proved under the random oracle model [3]. However, the scheme requires more pairing operations than the original scheme proposed in [1]. Zhang et al. [17] presented a CLS scheme with a formal security analysis but it still needs four pairing operations in the verification phase. Recently, Yap et al. [13] proposed a new CLS scheme, which requires no pairing operation in the signature phase but requires two pairing operations in the verification phase.

However, all the above CLS schemes use more than one pairing operations. Since pairing operations are quite expensive in computation and are usually time-consuming, these schemes are difficult to be applied for CPS as they constantly interact with the physical environments, hence CPS usually have stringent timing requirements. In this paper, we present McCLS scheme, which is more efficient and hence is a good candidate to be used in CPS.

A good security protocol must be resilient against security attacks. In the following, we briefly introduce two most commonly studied attacks. Later in this paper, we prove that the proposed McCLS scheme is resilient against these two attacks.

Black hole attack [8] is one of the many possible attacks in MANETs where a malicious node can attract all packets by falsely claiming a fresh route to the destination and then absorb them without forwarding them to the destination.

Rushing attack [6] usually aims at a reactive routing protocol. Every node in the network only forwards the first route discovery packet that it receives and drops the rest. If the attacker is able to reach the target first, before arrival of the legitimate Route Request, the attack can force a route through itself. In this way, the attacker is placed in an advantageous position.

3. Preliminaries

In this section, we present some mathematical background which helps in realizing CLS based on the bilinear pairing. It is commonly used in CLS schemes to realize signature and verification [1, 7].

We define two cyclic groups G_1, G_2 , where G_1 is an additive group and G_2 is a multiplicative group, where both groups have a prime order p . Let e be a computable bilinear map $e : G_1 \times G_1 \rightarrow G_2$. For $a, b \in \mathbb{Z}_p^*$ and $P, Q \in G_1$, we have $e(aP, bQ) = e(P, Q)^{ab}$. We also require non-degeneracy $e(P, Q) \neq 1$.

An efficiently computable bilinear map e provides an algorithm for solving the Decision Diffie-Hellman Problem (*DDHP*) [4]. That is, given $(P, aP, bP, cP) \in G_1$ and $a, b \in \mathbb{Z}_p^*$, decide whether $c \equiv ab \in \mathbb{Z}_p^*$.

The Computational Diffie-Hellman Problem (*CDHP*) is to compute $abP \in G_1$ when given (P, aP, bP) for $a, b \in \mathbb{Z}_p^*$. In bilinear pairing, Decision Diffie-Hellman Problem (*DDHP*) is easy and Computational Diffie-Hellman Problem (*CDHP*) is still hard. That is, for $a, b \in \mathbb{Z}_p^*$, given (P, aP, bP) , computing abP is infeasible. The *CDH* assumption states that there is no polynomial time algorithm with a non-negligible advantage in solving the *CDHP* [13].

3.1. Certificateless scheme and Adversarial Model

We omit this section for page limitation.

4. McCLS Scheme

McCLS scheme is motivated by the identity-based signature from [15], being an adaptation of the former to the certificateless setting. Our verification phase algorithm requires one pairing operation only, hence McCLS scheme outperforms the other existing CLS schemes in terms of efficiency. Besides, since McCLS scheme involves no pairing computation, messages signing is also efficient. McCLS scheme is comprised of the following five stages.

- **Setup.** Given a GDH group G_1 of order p , with an admissible pairing e and its generator P , pick $s \in \mathbb{Z}_p^*$ and set $P_{pub} = sP$. Choose two hash functions $H_1 : \{0, 1\}^* \rightarrow G_1$ and $H_2 : \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_p^*$. The public system parameter list is (P, P_{pub}, H_1, H_2) , and the master private key is s .
- **Extract Partial Private Key.** Given an identity ID , computes $Q_{ID} = H_1(ID)$ and $D_{ID} = sH_1(ID)$. Output D_{ID} as the partial private key corresponding to $Q_{ID} = H_1(ID)$.
- **Generate Key Pair.** Generate a secret $x \in \mathbb{Z}_p^*$. The public key is $P_{ID} = xP_{pub}$. The user's private key is $S_{ID} = x$.
- **CL-Sign.** Given the user's private keys (D_{ID}, S_{ID}) and a message M , pick a number $r \in \mathbb{Z}_p^*$ and output a signature $\sigma = (V, S, R)$ where $S = \frac{1}{S_{ID}}D_{ID}$, $R = (r - S_{ID})P$ and $V = H_2(M, R, P_{ID})r$.
- **CL-Verify.** Given the signature (V, S, R) of a message M for the identity ID , compute $h = H_2(M, R, P_{ID})$. Then check whether $(P_{pub}, VP - hR, S/h, Q_{ID})$ is a valid Diffie-Hellman tuple.

5. Analysis of McCLS Scheme

In this section, we analyze the correctness, performance and security proof of McCLS scheme.

5.1. Correctness

The correctness of McCLS scheme can be verified as follows:

$$\begin{aligned}
& e(VP - hR, S/h) \\
&= e(hrP - hrP + xhP, S/h) \\
&= e(xhP, D_{ID}/xh) \\
&= e(sP, Q_{ID}) \\
&= e(P_{pub}, Q_{ID}).
\end{aligned}$$

McCLS scheme only needs to compute pairing operation once since $e(P_{pub}, Q_{ID})$ is a constant. So McCLS scheme is more efficient than other previous schemes.

5.2. Security Proof

The main theorems concerning the security of our scheme are:

Theorem 1. *Our certificateless signature scheme is existentially unforgeable against a Type I adversary A_I in the random oracle model under the CDH assumption in G_1 .*

Proof. Suppose there exists an adversary A_I which has advantage in attacking McCLS scheme. We build a challenger C that uses A_I to solve the *CDH* problem. C receives an instance (P, aP, bP) of the *CDHP*. Its goal is to compute abP . On the setup phase, C sets P as the generator of the group, and sets $P_{pub} = aP$ where a is the master key, which is unknown to A_I . C then randomly chooses the target user identity ID^* , gives $(ID^*, params)$ to A_I and starts to answer oracle queries with the following procedures [12]:

- **H_1 Queries (ID_i).** If $ID_i = ID^*$, C saves the tuple $(ID_i, Q_i, P_i, y_i, x_i)$ where $Q_i = bP$, $P_i = xP_{pub}$, $x_i = x$, $x \in \mathbb{Z}_p^*$ and $y_i = \perp$ (indicate to failure). Otherwise, C generates a random y_i and lets $Q_i = y_iP$. Then C makes $P_i = x_i = \perp$, saves the tuple $(ID_i, Q_i, P_i, y_i, x_i)$ and returns $H_1(ID_i) = Q_i$.
- **Partial Key Extraction (ID_i) Queries.** When A_I makes the query on ID_i , C finds the tuple $(ID_i, Q_i, P_i, y_i, x_i)$. If the tuple does not exist, or $y_i = \perp$, then C aborts. Otherwise answer with $D_{ID_i} = y_iP_{pub} = y_i(aP)$. Note that A_I is not allowed to request the partial private key for ID^* .
- **Secret Value Extraction (ID_i) Queries.** When A_I makes the query on ID_i , C finds the tuple $(ID_i, Q_i, P_i, y_i, x_i)$. If it does not exist, or $y_i = \perp$, then C aborts. If $x_i = \perp$, C chooses a random $x_i \in \mathbb{Z}_p^*$ and saves its value. In any case, returns x_i .

- **Public Key Extraction (ID_i) Queries.** When A_I makes the query on ID_i , C finds the tuple $(ID_i, Q_i, P_i, y_i, x_i)$. If it does not exist, or $y_i = \perp$, then C aborts. If $x_i = \perp$, C executes **Secret Value Extraction Queries** to generate a private key. C replies with $P_i = x_i P_{pub}$. If $ID_i = ID^*$, C replies with $P_i = x P_{pub}$.
- **Public Key Replacement(ID_i, P'_i) Queries.** When A_I makes the query on (ID_i, P'_i) , C finds the tuple $(ID_i, Q_i, P_i, y_i, x_i)$. If it does not exist, C aborts. Otherwise C sets $x_i = \perp$ and $P_i = P'_i$.
- **H_2 Queries (ID_i).** When A_I make the query on (M_j, R_j, P_i) , If not defined, C picks a random $h_j \in \mathbb{Z}_p^*$ as the hash value and returns $H_2(M_j, R_j, P_i) = h_j$.
- **Sign Queries(ID_i, M_j).** When A_I asks for a signature by user ID_i on message M_j . Note that if $ID_i \neq ID^*$, A_I is able to generate signature on any messages using corresponding private keys. As far as $ID_i = ID^*$, assume that P_i is current public key and corresponding private key additionally submits through the A_I . Because the public key has been replaced earlier by A_I , then C cannot know the corresponding private key and thus the signing oracle's answer may not be correct. On receiving sign queries, C does the following:

1. Choosing random $r_j, h_j \in \mathbb{Z}_p^*$;
2. Computing $V_j = h_j(x + \frac{a}{r_j})$ and $S_j = r_j Q_i = r_j bP, R_j = xP$;
3. If $H_2(M_j, R_j, P_i) = h_j$ is defined, return \perp ; otherwise, setting $H_2(M_j, R_j, P_i) = h_j$;
4. Returning the signature $\sigma = (V_j, S_j, R_j)$.

Finally, A_I will output a valid forgery $r = (ID_j, M_j, R_j, S_j, V_j)$. If $ID_j \neq ID^*$, C output the FAIL and aborts the simulation. Otherwise, we can compute r through $r_j = \frac{ah_j}{V_j - h_j x}$, since $(P_{pub}, V_j P - h_j R_j, S_j / h_j, Q_i)$ is a valid Diffie-Hellman tuple. Apply r_j to S_j , we have

$$S_j = \frac{ah_j}{V_j - h_j x} Q_i$$

$$S_j = \frac{ah_j}{V_j - h_j x} bP$$

$$abP = S_j (V_j - h_j x) / h_j \quad .$$

So $abP = S_j (V_j - h_j x) / h_j$ is the answer to our CDHP instance. If the A_I can break our scheme, then the attacker solves the CDH problem.

Theorem 2. *Our certificateless signature scheme is existentially unforgeable against the A_{II} adversary in the random oracle model under the CDH assumption in G_1 .*

We cannot present the detailed proof here due to the page limitation. In the full version of the paper, the proof of Theorem 2 will be presented.

5.3. Performance

McCLS scheme only requires two scalar multiplication in signature phase and two scalar multiplication computations and one pairing operation in verification phase. The pairing operations are more expensive compared to scalar multiplication and exponentiation. The comparison of the exiting schemes and McCLS scheme according to efficiency of signature and verification algorithms and the length of public keys is shown in Table 1. We can see that McCLS scheme has the lowest pairing operations requirement and has the same length of public key with other CLS schemes.

Table 1. Comparison of the CLS Schemes

	AP [1]	ZWXF [17]	YHG [13]	McCLS
Sign	1p+3s	4s	2s	2s
Verify	4p+1e	4p+3s	2p+3s	1p+1s
PubKey Len	2 points	1 points	1 point	1 point

s : the scalar multiplication computation;

p : the pairing operation;

e : the exponential computation.

6. Evaluation

A simulation based on QualNet [10] has been conducted to test the performance of McCLS. Our implementation retains most of the Ad hoc On-Demand Distance Vector Routing (AODV) mechanisms, such as route discovery, reverse path setup, forwarding path setup, route maintenance, and so on. We conduct the simulations in order to compare the original AODV scheme without any security requirements and McCLS scheme based on the CLS with routing authentication extension. Besides, the performance of two schemes was evaluated under 2 nodes *black hole attacks* and 2 nodes *rushing attacks*. In our experiments, 20 nodes move around in a rectangular area of 900×900m according to the random waypoint model. The nodes are spread randomly over the network and each node starts its journey from a random location to a random destination. We vary the nodes speed from 0m/s to 20m/s, and set the nodes pause time to 0s.

The performance of McCLS is compared AODV using the following performance metrics.

- **Packet Delivery Ratio:** Ratio of the number of packets received by the destination to the number of packets sent by the source.
- **RREQ Ratio:** Ratio of the total number of RREQ initiated, forwarded and retried to the total number of data packets sent as source and data packets forwarded.

- End-to-End Delay: The average time experienced by each packet when traveling from the source to the destination.
- Packet Drop Ratio: Ratio of the number of packets discarded by attack nodes to the total number of packets sent by all sources.

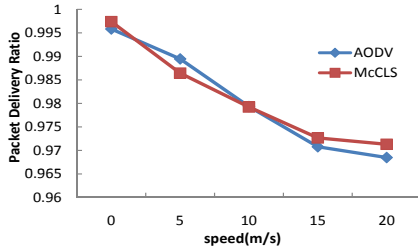


Figure 1. Packet Delivery Ratio

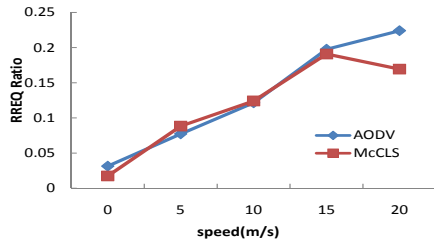


Figure 2. RREQ Ratio

Packet delivery ratio and the RREQ ratio is shown in Fig.1 and Fig.2, respectively. As one can see McCLS scheme could work well in the experiment. The packet delivery ratio and RREQ ratio for AODV are very similar with McCLS scheme, without causing any substantial degradation of the network performance. As nodes speed increases, the data packets reaching to the destination decrease and the RREQ packets transmitting through the networks increase.

End-to-end delay of McCLS scheme is shown in Fig.3. McCLS scheme has a little bit higher delay than AODV due to the exchange of packets during signature and verification phase of the security process. The result shows that McCLS scheme has a similar end-to-end delay with AODV at a relatively low speed, however, when the maximum speed of nodes is higher than 15m/s, AODV outperforms McCLS scheme. To explain this, McCLS scheme needs one pairing operation and two scalar multiplication computations, and those additional operations are computed in McCLS but not in AODV scheme.

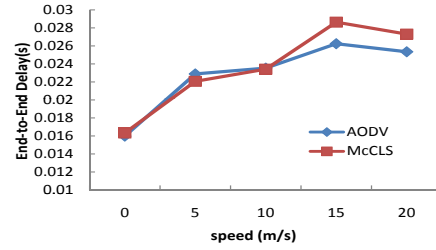


Figure 3. End-to-End Delay

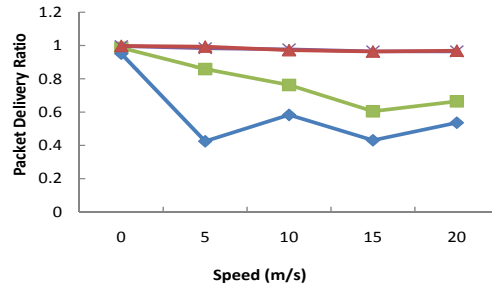


Figure 4. Packet Delivery Ratio

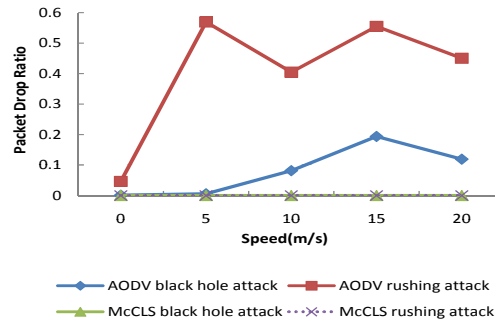


Figure 5. Packet Drop Ratio

Packet delivery ratio under *black hole attack* is shown in Fig.4. From the results, we can see that packet delivery ratio drops as the speed increases when we use AODV routing protocol under *black hole attack*. Similarly, when the network under *rushing attack*, the packet delivery ratio decreases remarkably. Especially, the packet delivery ratio drops to 43% at speed of 5m/s under the two nodes *rushing attack*. However, McCLS scheme is similar in packet delivery ratio with AODV routing protocol before under the *black hole attack* and *rushing attack*. Packet drop ratio is

shown in Fig.5. When we have the 2 nodes *black hole attack* and *rushing attack*, the highest packet dropped ratio of AODV routing protocol is almost 19% at speed of 15m/s and 57% at speed of 5m/s respectively. On the contrary, McCLS scheme is able to detect all *black hole attack* and *rushing attack* and the packet drop ratio is zero. Therefore, the proposed McCLS scheme can effectively resist such attacks.

7. Conclusion

An efficient certificateless signature scheme named McCLS based on the bilinear Diffie-Hellman assumption in the random oracle model for mobile wireless cyber-physical systems is proposed in this paper. Our signature phase and verification phase require none and one pairing operation respectively, which is more efficient than other existing certificateless signature schemes. We present simulation results of McCLS scheme and compare the performance under two most common attacks (*black hole attack* and *rushing attack*) to a typical routing protocol-AODV, where no protect mechanism is provided. Results show that the scheme is more efficient and resists these two kinds of attacks.

Acknowledgment

This work was supported in part by an NSERC discovery grant 341823-07 and a National Study-Abroad Scholarship of P.R.China under Grant No. [2007] 3020.

References

- [1] S. S. Al-Riyami and K. G. Paterson. Certificateless Public Key Cryptography. In *ASIACRYPT: Advances in Cryptology – ASIACRYPT: International Conference on the Theory and Application of Cryptology*. LNCS, Springer-Verlag, 2003.
- [2] M. Anand, E. Cronin, and M. Sherr. Security Challenges in Next Generation Cyber Physical Systems. Technical report, University of Pennsylvania, 2007. <http://www.truststc.org/scada/papers/paper33.pdf>.
- [3] M. Bellare and P. Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. In *1st ACM Conference on Computer and Communications Security*, pages 62–73, 1993.
- [4] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In *Advances in Cryptology - CRYPTO 2001: 21st Annual International Cryptology Conference*, volume 2139, pages 213–229. LNCS, 2001.
- [5] H. Deng, A. Mukherjee, and D. P. Agrawal. Threshold and Identity-Based Key Management and Authentication for Wireless Ad Hoc Networks. In *International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004*, pages 107–111, April 2004.
- [6] Y.-C. Hu, A. Perrig, and D. B. Johnson. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. In *Proc of the ACM Workshop on Wireless Security (WiSe 2003)*, pages 30–40, 2003.
- [7] X. Huang, W. Susilo, Y. Mu, and F. Zhang. On the Security of Certificateless Signature Schemes from Asiacrypt 2003. In *International Conference on Cryptology and Network Security (CANS), LNCS*, volume 4, 2005.
- [8] S. Marti, T. Giuli, K. Lai, and M. Baker. Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MOBICOM-00)*, pages 255–265, 2000.
- [9] National Science Foundation. Cyber-physical systems. Technical report, NSF Workshop on Cyber-Physical Systems, 2006. <http://varma.ece.cmu.edu/cps/>.
- [10] Scalable Network Technologies. QualNet Simulator. <http://www.scalable-networks.com/>.
- [11] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In *CRYPTO: Proceedings of Crypto*, 1984.
- [12] S. Xu, Y. Mu, and W. Susilo. Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security. In *11th Australasian Conference on Information Security and Privacy, ACISP 2006*. LNCS, 2006.
- [13] W.-S. Yap, S.-H. Heng, and B.-M. Goi. An Efficient Certificateless Signature Scheme. In *EUC Workshops*, volume 4097 of *Lecture Notes in Computer Science*, pages 322–331, 2006.
- [14] S. Yi and R. Kravets. Moca: Mobile Certificate Authority for Wireless Ad Hoc Networks. In *Proc. Second Ann. PKI Research Workshop (PKI '03)*, Apr 2003.
- [15] H. Yoon, J. H. Cheon, and Y. Kim. Batch Verifications with ID-Based Signatures. In *ICISC: International Conference on Information Security and Cryptology*. LNCS, 2004.
- [16] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon. AC-PKI: Anonymous and Certificateless Public-key Infrastructure for Mobile Ad Hoc Networks. In *2005 IEEE International Conference on Communications, 2005. ICC 2005*, pages 3515–3519, May 2005.
- [17] Z. Zhang, D. S. Wong, J. Xu, and D. Feng. Certificateless Public-Key Signature: Security Model and Efficient Construction. In *Applied Cryptography and Network Security, 4th International Conference, ACNS 2006, Singapore, June 6-9, 2006, Proceedings*, volume 3989 of *Lecture Notes in Computer Science*, pages 293–308, 2006.
- [18] L. Zhou and Z. Haas. Securing Ad Hoc Networks. *Network, IEEE*, 13(6):24–30, Nov/Dec 1999.