Identity Based Authentication using a Cross Layer Design approach in Wireless Sensor Networks

Harsh Kupwade Patil
Department of Computer Science
Southern Methodist University
Dallas, Texas. USA
Email: hkupwade@smu.edu

Joseph Camp
Department of Electrical Engineering
Southern Methodist University
Dallas, Texas, USA

Stephen A. Szygenda
Department of Computer Science
Southern Methodist University
Dallas, Texas. USA

***Abstract*— The development of Wireless Sensor Networks (WSN) was originally motivated for military applications such as battlefield surveillance. However, in recent years it has gained popularity in many civilian applications: such as habitat monitoring, healthcare, home automation, traffic control and environmental monitoring. As more low cost, low power and multifunctional sensor nodes are being deployed, security in such sensor networks become one of the prominent issues in WSN. Recent advances in wireless networks did not give the necessary attention to security with regard to device constraints, since they base their design on legacy wireless networks. As more security solutions are being proposed in WSN, there is an increase in the lack of co-ordination between various security measures at different layers, leading to functional redundancy and increased overhead. As WSN scale to a very large number, current malicious node detection schemes will be resource intensive and inefficient Therefore, new approaches are being sought to efficiently use information from different protocol layers to propose security. They not only focus on layer interactions within a node, but also adapt to changes in the network conditions and adaptively optimize cross-layer interactions across different nodes. It has been shown that pairing based crypto operations are possible on sensor nodes (motes) and a completely new security suite is being developed for WSN using Identity based Cryptography. In this paper, we propose a new cross-layer design approach for WSN using Identity based cryptography. This approach combines cross-layer design principles along with Identity based Cryptography to provide a new set of security solutions, which could be more efficient in storage, computation and energy.**

I. Introduction

Wireless Sensor Networks (WSN) has been one of the most promising solutions to many applications and security in these networks is crucial to WSN [1]. A typical sensor network consists of computationally limited low cost sensors that can scale from a few hundreds to thousands in number. Besides incorporating the basic vulnerabilities in ad-hoc networks, WSN pose new challenges such as survivability (physical access to adversaries) and lesser computational power than the conventional ad-hoc networks. Many scalable and efficient security solutions have been proposed to improve the energy efficiency in WSN and one approach among them is Elliptic Curve Cryptography (ECC) [2],[3]. Given the limited computational power and the resource constrained nature of wireless sensors, [2] has shown considerable reduction in memory access and computational time in key agreement by efficiently implementing binary field algorithms such as squaring, multiplication, inversion and modular reduction on Micaz mote. [3] has implemented pairing based signature (BLS-SS [4] and BB-SS[5]) and encryption schemes (BF-IBE [6]) on the MICA family, and has shown that it achieves faster computation and lower memory consumption by choosing super-singular elliptic curve as a pairing group.

However, one of the main commonality with these protocols is that they abide by the traditional layered architecture. Although they may achieve a very high performance in their assigned specific layers, a cross layer approach for digital signature generation and key distribution can jointly optimize and increase the overall network security in WSN. It has been observed that the modular approach to the development of security protocols for individual layers might provide redundant security services and hence consume more energy than required in WSN. In some situations, an over-engineered security design may exhaust all the energy resources, leading to a security service denial of service attack. For example, the non-adaptive nature of the security service can be ineffective in preventing the more sophisticated attacks that look for vulnerabilities at each layer. For example, security provisioning at the network layer can be ineffective since the attacker can spoof the target's MAC address and launch a Denial of Service (DoS) attack. In this paper, we look at a new cross-layer approach to authentication using pairing based cryptography.

II. Related Work

1) Identity based cryptography:

a) Overview: In 1984, Shamir introduced Identity Based Cryptography (IBC) [16]. He could construct an Identity Based Signature (IBS) scheme using the existing RSA function [17], but was unsuccessful in constructing an Identity Based Encryption (IBE) scheme and it remained a long standing problem for almost a decade. In 2001, Boneh and Franklin came up with an independent solution using the concept of bilinear maps [6]. It led to a new era of research where many identity based digital signature schemes were proposed using bilinear maps. At the same time, Cocks proposed an Identity Based Encryption (IBE) scheme using quadratic residuosity [7]. However, Cock's scheme is limited in its applicability

to WSN due to the generation of long ciphers and slower performance as it is based on ternary quadratic form.

In IBC, an end user can choose an arbitrary string to be his identity. This identity is used in generating the public key. Therefore, they do not need digital certificates from Certificate Authorities (CA) to verify digital signatures. A trusted third party Private Key Generator (PKG) is responsible to distribute private keys corresponding to their identity (Figure 1).

b) Key Distribution in IBE: The general key distribution problem refers to the onerous task of distributing secret keys between communicating parties to provide security properties such as authentication or confidentiality or both. But with the advent of private key distribution, new problems arise such as the inherent key escrow problem and the need for secure distribution of private keys [22].

Alice **PKG (Private Key Generator)** **Bob**

1. Request for Private Key →

← 2. Private Key

3. Digital Signature/Encryption →

Figure 1: Key distribution in Identity Based System

Byoungcheon Lee *et. al* came up with a secure scheme for private key distribution in IBC. We briefly review [22].

Let H_1, H_2 and H_3 be three hash functions such that

$$H_1 : \{0,1\}^l \rightarrow G_1 \tag{1}$$

where l is the length of the plain text.

$$H_2 : \{0,1\}^l \times G_2 \rightarrow Z_q \tag{2}$$

$Z_q = Z/qZ$ denotes integers $\bmod q$ where q is a large prime. Therefore Z_q denotes the group $\{0, 1, 2, ..., q-1\}$ and $Z_q^* = Z \backslash \{0\}$.

$$H_3 : G_2 \rightarrow Z_q^* \tag{3}$$

The PKG specifies two groups $G_1$and G_2 of order q, where G_1 is an additive group and G_2 is a multiplicative group. Let e be a bilinear map such that $e : G_1 \times G_1 \rightarrow G_2$ with the following properties

- Bilinear: Let $(x_1, x_2$ and $y) \in G_1$. Then

$$e(x_1 + x_2, y) = e(x_1, y).e(x_2, y) \tag{4}$$

- Non-degenerate: There exists $x \in G_1$ and $y \in G_1$ such that

$$e(x, y) \neq 1 \tag{5}$$

In fact G_1 is a point subgroup on an elliptic curve over a finite field and G_2 is a subgroup of a cyclic group of a larger finite field. The pairings are derived from the Weil, Tate or η_T pairing [6], [8]. The PKG chooses a private key $s_0 \in Z_q^*$ and computes the master public key

$$P_0 = s_0 P \text{ where } P \in G_1 \tag{6}$$

The security of the master public key is dependent on the elliptic curve discrete log problem [18]. The PKG publishes the description of the groups G_1 and G_2, public key P_0, hash functions $(H_1, H_2$ and $H_3)$,the bilinear map e and the group element P. Alice and Bob choose their secrets to compute their blinding factors. Alice with identity ID_A chooses a random secret $x \in Z_q^*$ and computes a blinding factor $X = xP$. An eavesdropper will not be able to generate the private key since he has no knowledge of the secret x. She then requests the PKG to issue a partial private key by sending X and ID_A. The PKG would use some pre-shared credentials to verify the authenticity of an end user's identity.

The PKG validates Alice's identity and computes the public key of Alice as

$$Q_{ID_A} = H_1(ID_A) \tag{7}$$

It computes a blinded partial private key as

$$Q_{bl_A} = H_3[e(s_0 X, P_0)] s_0 Q_{ID_A} \tag{8}$$

It then generates a signature $Sig(Q_{bl_A})$ for providing integrity protection.

$$Sig(Q_{bl_A}) = soQ_{bl_A} \tag{9}$$

It sends $Sig(Q_{bl_A})$ and Q_{bl_A} to Alice.

Alice verifies the signature using the below mentioned formula,

$$e(Sig(Q_{bl_A}), P) \stackrel{?}{=} e(Q_{bl_A}, P_0) \tag{10}$$

and finally retrieves her private key D_{ID_A} by un-blinding Q_{bl_A}as follows

$$D_{ID_A} = \frac{Q_{bl_A}}{H_3[e(P_0, P_0)^x]} \tag{11}$$

Hence there is a secure key exchange between the PKG and the end users. Identity based authentication can be easily extended to a two level hierarchical domain environment as shown in figure 2.

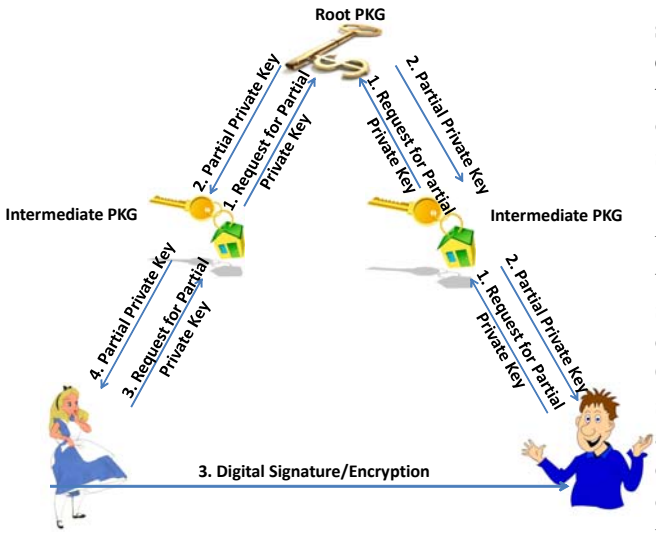

Figure 2: Identity based authentication in a two level hierarchical environment

Alice would then use Gentry and Silverberg's algorithm to generate a digital signature or Chow *et al's* algorithm to generate a signcrypted message [25],[26]. Signcrypted messages can only be verified by the intended recipient as he would use his own private key along with sender's public key to validate the ciphertext. Concerning the key escrow problem, one of the promising approaches is in using threshold key cryptography in which one full piece of secret information is derived from a set of secret shares [19],[20]. [6] directly apply the techniques of threshold key cryptography to their IBE systems. The master secret $s_0 \in Z_q^*$ is used to generate the private key $D_{ID} = s_0 Q_{ID}$, where Q_{ID} is derived from the user's public key identity. This private key can be easily distributed in a $t-$outof$-n$ fashion by giving each of the n-PKGs one share s_i of the secret s. When generating the private key each of the t chosen PKGs simply respond with $D^{(i)}_{ID_{priv}} = s_i Q_{ID}$. The user can then construct $D_{ID_{priv}}$ as $D_{priv} = \Sigma \lambda_i D^{(i)}_{ID_{priv}}$ where λ_i are the appropriate Lagrange coefficients.

c) Accountable Authority Identity based Encryption (A-IBE): A-IBE is a variant of the IBE scheme having an exponential or super-polynomial number of possible decryption keys available corresponding to every identity. Each decryption key d_{ID} for an identity will belong to a unique decryption key family (denoted by the number nF). Roughly speaking, in the definitions of security we will require that: given a decryption key belonging to a family, it should be intractable to find a decryption key belonging to a different family (although it may be possible to find another decryption key belonging to the same family). The end user gets the decryption key corresponding to his identity from the PKG using a secure key generation protocol [22]. The protocol allows the user to obtain a single decryption key d_{ID} for his identity without letting the PKG know which key he obtained. If the PKG turns malicious and generates a decryption key $d^{'}_{ID}$ for that specific identity, with all but negligible probability, it will be different from the key, which the end user obtained. Therefore the generation of a key pair (d_{ID},$d^{'}_{ID}$) is a cryptographic proof of malicious behavior of the PKG as only one key per identity should be used in circulation.

d) Key Distribution in WSN: The traditional key distribution mechanism based on Public Key Infrastructure (PKI) would be impractical in WSN due to the increase in consumption of energy [15]. A more pragmatic approach to key distribution in WSN is by relying on pre-key distribution. One of the approaches to pre-key distribution is by using a single pre-key distribution for the entire sensor network. This approach would be inefficient if any of the sensor nodes is captured by an adversary and would lead to the compromise of the entire network. To avoid the compromise of the entire network, the other approach is to setup a pair-wise key sharing between every two sensor nodes. Therefore every node will have $n-1$ keys and the entire network will have $\frac{n(n-1)}{2}$ keys. One of the major disadvantages with this approach is that the entire network has to be re-keyed if new nodes are added into the network or with the deletion of existing nodes. In addition, storage of $n-1$ keys in every sensor node will be resource intensive.

Eschenauer and Gligor proposed a new centralized key management scheme called as the basic random key scheme [9]. It consists of three phases.

Phase I: Key Pre-distribution

Each sensor stores keys in the form of a key-ring. The ring consists of randomly chosen k keys from a large pool of keys. Each key in the key-ring has a key identifier which is stored in the sensor. Further, each sensor node i would share a pairwise key K with its corresponding base station. The scheme is weakened if the base station within the domain were compromised.

Phase II: Shared key discovery

Each sensor discovers its neighbors who are in the communication domain by simply broadcasting a list of identifiers for its corresponding keys in an un-encrypted fashion. However, a malicious neighboring node can easily eavesdrop on the key sharing pattern among other sensors within the communication domain. They propose a challenge response mechanism for secure sharing of keys among nodes, which is computationally intensive.

Phase III: Path key establishment: A path key is established at the end of the shared key phase between the two communicating nodes. The topology for the sensor array as seen by the network layer (routing layer) is set by the end of phase II. However, it would hamper routing as a path key between nodes has to be established between end-to-end communicating parties. Revocation is inefficient, as the base station has to send a message to all the nodes within the communication domain to revoke the compromised key.

III. Identity Based Authentication using Cross Layer Domain.

In 1997, Zheng showed that by combining authentication with encryption into a single primitive, it was possible to achieve significant savings on both communication and computational overhead [14]. Implementing signcryption schemes in WSN would be advantageous as the end users verify the sender's identity as well as decrypt messages at the same time. Below we briefly review two important signcryption schemes and its applicability in WSN.

A. Lynn's algorithm [24]

Let

$$H_4 : \{0,1\}^* \times \{0,1\}^* \rightarrow Z_q \tag{12}$$

$$H_5 : Z_q \times G_2 \rightarrow \{0,1\}^* \tag{13}$$

$$H_6 : \{0,1\}^l \rightarrow \{0,1\}^* \tag{14}$$

Alice would pick a random secret $k \in Z_q^*$ and compute

$$q = H_4(k, m) \text{ where } m \text{ is the message} \tag{15}$$

and

$$w = e(D_{ID_A}, Q_{ID_B}) \tag{16}$$

Alice would then send the signcrypted message $\prec U, V, W \succ$ to Bob where

$$\prec U, V, W \succ \;=\; \prec q, En_{H_5[q,w]}(k), En_{H_6[k]}(m) \succ \tag{17}$$

$En_{(Key)}$ refers to encryption using AES algorithm [29].
Bob would decrypt the message m as shown below

$$e(Q_{ID_A}, D_{ID_B}) = w \tag{18}$$

$$Dn_{H_5[U,w]}(V) = k \tag{19}$$

$$Dn_{H_6[k]}(W) = m \tag{20}$$

B. Chow et al's algorithm [26]

Let us consider a WSN network consisting of a sink node (node with abundant resources) along with a few cluster nodes. The sensor nodes send sensed data to their respective cluster nodes, which may aggregate the data and further send it to the sink node.

Subsequently, let domain one be controlled by the root PKG (Sink Node) and domain two be controlled by the cluster nodes.

Let the Root PKG's master private key be $M_s \in Z_q^*$ and the master public key be $Q_0 = M_s P$ where $P \in G_1$. Let $s_1 \in Z_q^*$ then

$$Q_1 = s_1 P \tag{21}$$

where Q_1 is a public parameter generated by one of the cluster nodes.

$$H_7 : G_2 \rightarrow \{0,1\}^* \tag{22}$$

Alice would generate the signature

$$\mathrm{Si}\, g_c = D_{ID_A} + kP_M \tag{23}$$

where $P_M = H_1(m)$
and compute

$$g = e(Q_0, kQ_{ID_2}) \tag{24}$$

She would generate the signcrypted message as shown below,

$$\prec, \overbrace{kQ_{ID_B}}^{U_1}, \overbrace{En_{H_7[g]}(m||\,\mathrm{Si}\, g_c||ID_B)}^{V}, \overbrace{Q_0}^{W_1}, \overbrace{Q_1}^{W_2}, \overbrace{Q_M}^{W_3} \succ \tag{25}$$

where $Q_M = kP$.
Alice would send $\prec U_1, U_2, V, W_1, W_2, W_3 \succ$ to Bob.
Bob would compute

$$\frac{e(W_3, D_{ID_B})}{e(Q_2, U_1)} = g \tag{26}$$

and then decrypt V as shown below,

$$Dn_{H_7[g]}(V) = (m||\,\mathrm{Si}\, g_c||ID_B) \tag{27}$$

He would then verify the signature as shown below,

$$\frac{e(P, \mathrm{Si}\, g_c)}{e(W_2, Q_{ID_A})} \stackrel{?}{=} e(W_1, Q_{ID_1}) e(W_3, P_M)$$

In case of authentication, we could apply Hess's Identity based signature scheme in WSN [23]

The use of Identity field should not be restricted to the upper 3 layers (Application, Network and Data Link) and should also take the physical layer parameters as identities for authentication. Figure 3 describes the possible identity fields in different layers.

Layer	Identity Header
Application	Device Name
Network	IP address
Data Link	MAC address
Physical	Channel frequency response

Figure 3: Identity field at different layers

The conventional approach to assigning security to the upper layers would leave a gap between the upper and lower layers (physical layer). An unsecured physical layer is susceptible to a broad range of security attacks. Therefore the physical layer properties in a wireless medium have to be leveraged to address the security threats. A legitimate user can be differentiated from a rogue end user by measuring the channel frequency response and hypothesis testing [32].

On the contrary, solely depending on the physical layer is not the best approach to providing security. The traditional security schemes in the physical layer (Frequency Hopping Spread Spectrum or Direct Sequence Spread Spectrum) could be rendered insecure, if the intermediate adversary along the active routing path has prior knowledge of the hopping pattern or the spreading code. In such cases an adaptive, location and energy efficient cross layer design approach should be adopted to provide a holistic security solution.

We suggest that the identity field should not be fixed to a specific layer and should opt for a cross layer approach, wherein the end user decides the identity depending on the type of authentication mechanism (hop-by-hop or end to end). Figure 4 shows end-to-end vs hop-by-hop authentication.

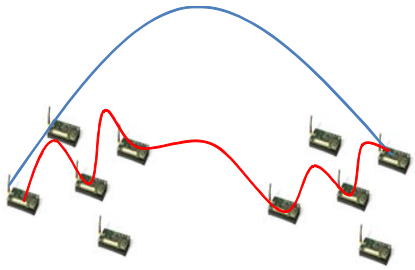

Figure 4: End -to-end Vs hop-by-hop authentication

In case the end user decides for end-to-end authentication in a network and if one of the intermediate nodes is compromised, the usual tendency of the end user is to wait till the timer expires and retransmits the digitally signed message via the same route. If the compromised sensor decides to drop all packets and distribute spurious routing tables to its neighbors, it will lead to a total compromise of the entire network. In such situation an adaptive authentication scheme would be beneficial as it would detect the malicious intermediate node by adapting from end-to-end authentication to hop-by-hop authentication. In addition, it would also increase the efficiency of the routing scheme of the entire network, as it will help un-compromised intermediate nodes to re-route the packets in an intelligent manner. If an end user would want to perform end-to-end authentication and send confidential information in WSN, a signcryption scheme would be more suitable as end users will be able to verify digital signatures and decrypt data in one operation. This scheme would fit the WSN environment as it would save the bandwidth and the battery life of the communicating sensors.

Additionally, the use of signcryption schemes will be beneficial in location and energy aware routing. Let us consider a WSN network, where the sink node has an inbuilt Global Positioning System (GPS) chip and is able to locate its position. Subsequently, all the other nodes are able to locate their position with reference to the sink node. Hence, each node is aware of its immediate neighbor's location and as well as the sink node. If the network adapts to a hop-by-hop signcryption scheme, each node could send its location co-ordinates and its energy levels in a signcrypted fashion, leading to intelligent location and energy aware routing.

The security of the network could be strengthened if the network and data-link identities could be concatenated using Unique Universal IDs (UUIDs) [31]. Application level identities can also be concatenated using UUIDs.

Concerning ID based key distribution schemes in WSN, a PKG could be a single entity who could be able to distribute private keys or it could be a group of sensor nodes (in a distributed architecture) acting as a PKG and the security would be based on threshold key cryptography. Although Accountable IBE is a promising approach in a centralized architecture, where the PKG could be held accountable in case it leaks the end user's key for an identity, its applicability in the WSN is restricted and would be totally inefficient in an ad-hoc environment. Key revocation is also possible if a collected group of sensor nodes vote against a sensor node, and if the number of votes against the sensor node exceeds a specific threshold, the node will be revoked [30]. However, this scheme would be inefficient if all the nodes that vote were compromised and could vote against an honest node; thereby compromising the entire network. The ease of developing short new identities at any layer offers huge operational advantages in resource constrained environments such as WSN. Paradoxically, the problem of key escrow is disadvantages with its applicability to public domains, but would be advantages in case of military applications in which an ad-hoc group moderator would want to monitor traffic between communicating parties.

IV. Conclusion

As WSN are expected to proliferate in large numbers in the coming decade, security would play a vital role in the smooth running of these networks. However, these networks pose a unique challenge within security domain due to the traditional layered security scheme. In this paper, we make an early attempt to combine the cross layer approach with the identity based authentication schemes using pairing based cryptography to open a new paradigm of security solutions. As more and more security proposals are being proposed in WSN using pairing based cryptography, to maximize efficiency in computation and energy consumption, a fusion with the cross layer approach will help in providing better routing schemes, revocation mechanisms, immediate detection of sophisticated cross layer attacks and network survivability. The lightweight nature of Tinypbc (Pairing based cryptography library for WSN) would take less than 10% of RAM and about 20% of ROM on a Micaz mote, which would leave plenty of space to run reasonably heavy applications such as the identity based signature/signcryption schemes. In addition, we show that ID based authentication schemes are not only computationally efficient, but can also be used in making intelligent location and energy aware routing decisions.

References

[1] X. Du and H. Chen , "Security in wireless sensor networks," IEEE Wireless Communications, vol. 15, issue 4, pp 60-66, Aug. 2008

[2] D. F. Aranha, R. Dahab, J. López, L. B. Oliveira, " Efficient implementation of elliptic curve cryptography in wireless sensors" Advances in Mathematics of Communications, vol. 4, issue 2, pp. 169-187, 2010.

[3] X. Xiong, D. S. Wong and X. Deng, "TinyPairing: A Fast and Lightweight Pairing-based Cryptographic Library for Wireless Sensor Networks," in *IEEE Wireless Communications and Networking Conference*, pp 1-6, April 2010.

[4] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the Weil pairing," in *Advances in Cryptology – ASIACRYPT 2001*, pp. 514-532, 2001.

[5] D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," Journal of Cryptology, Springer-Verlag, vol. 21(2), pp.149–177, 2008

[6] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology – CRYPTO 2001*, LNCS 2139, pp.213-229, 2001.

[7] C. Cocks, "An Identity Based Encryption Scheme Based on Quadratic Residues, Cryptography" in *Coding - Institute of Mathematics and Its Applications International Conference on Cryptography and Coding - Proceedings of IMA 2001*, LNCS 2260, pp 360-363, Springer-Verlag, 2001.

[8] S. D. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate Pairing," in Lecture Notes in Computer Science (LNCS), vol. 2369, pp 69-86, Springer Berlin, 2002

[9] L. Eschenauer and V. D. Gligor, " A key-management scheme for distributed sensor networks," in *CCS 02: Proceedings of the 9th ACM conference on computer and communication security*, pp 41-47, 2002.

[10] R. Ramanathan and J. Redi, " A Brief Overview of Ad Hoc Networks: Challenges and Directions", *IEEE Communication. Mag*., vol 40, no 5, pp 20-22, 2002.

[11] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical En-route Filtering of Injected False Data in Sensor Networks" IEEE Journal in Selected Areas in Communication, pp 839-850, 2005.

[12] M. Xiao, X .Wang and G. Yang, "Cross-Layer Design for the Security of Wireless Sensor Networks," in *Proceedings of the 6th World Congress on Intelligent Control and Automation*, vol 1, pp 104-108, 2006.

[13] D.J Malan, M. Welsh and M.D Smith "A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography" in *IEEE SENCON*, pp 71-80, 2004.

[14] Y. Zheng, "Signcryption and Its Applications in Efficient Public Key Solutions," in *Proceedings of Information Security Workshop*, 1997, LNCS, vol. 1397, Springer-Verlag, pp. 291-312, 1998.

[15] R. Housley, W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," IETF RFC 2459..

[16] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," in *Advances in Cryptology: Proceedings of CRYPTO* 84, Lecture Notes in Computer Science, vol. 196, Springer-Verlag, pp. 47-53, 1984.

[17] R. L. Rivest, A. Shamir, and L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,", Communications of the ACM , vol. 21, pp. 120-126, ACM NY, 1978.

[18] N.P. Smart, "The Discrete Logarithm Problem on Elliptic Curves of Trace One," *Journal of Cryptology*, vol. 12, Springer New York, pp. 193-196, 1999.

[19] P. Gemmell, "An introduction to threshold cryptography", in CryptoBytes, a technical newsletter of RSA Laboratories, Vol. 2, No. 7, 1997.

[20] R. Gennaro, S. Jarecki, H. Krawczyk, T. Rabin, "Secure Distributed Key Generation for Discrete-Log Based Cryptosystems", *Advances in Cryptology - Eurocrypt '99*, Lecture Notes in Computer Science, Vol. 1592, Springer-Verlag, pp. 295-310, 1999.

[21] V. Goyal, S. Lu, A. Sahai and B. Waters, "Black-Box Accountable Authority Identity Based Encryption", in *ACM Conference on Computer and Communications Security*, pages 89–98. ACM, 2008.

[22] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure Key Issuing in ID-based Cryptography," in *Conferences in Research and Practice in Information Technology*, 2004, vol. 32, pp. 69-74.

[23] F. Hess, "Efficient Identity Based Signature Schemes based on Pairings," in *Selected Areas in Cryptography: 9th Annual International Workshop*, 2002, LNCS, vol. 2595, Springer-Verlag, pp. 310-324, 2003

[24] B. Lynn, "Authenticated Identity-Based Encryption," available at http://eprint.iacr.org/2002/072/.

[25] A. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," in *Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security*, 2002, LNCS, vol. 2501, Springer-Verlag, pp. 548 - 566, 2002.

[26] S. Chow , T. Yuen, L. Hui and S. Yiu, "Signcryption in Hierarchical Identity Based Cryptosystem," *Security and Privacy in the Age of Ubiquitous Computing, International Federation for Information Processing,* vol. 181, pp. 443-457, Springer Boston, 2005

[27] Secure Hash Standard availabe at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf.

[28] S. Josefsson, "The Base16, Base32, and Base64 Data Encodings," IETF RFC 3548, July 2003.

[29] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001, available at *http://www.itl.nist.gov/fipspubs/*.

[30] H. Chan, V. Gligor, A. Perrig, and G. Muralidharan, "On the distribution and revocation of cryptographic keys in sensor networks," IEEE Transactions on Dependable and Secure Computing, vol. 2, no. 3, pp 233-247, July-Sept. 2005

[31] P. Leach, M. Mealling and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace," IETF RFC 4122, July 2005.

[32] L. Xiao, L. J. Greenstein, N. B. Mandayam and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels" in IEEE Transactions on Wireless Communications, vol. 7, No. 7, pp. 2571-2579, July 2008

[33] D. F. Aranha, "Tiny Pairing-based Cryptography Library," available at *http://code.google.com/p/relic-toolkit/*

[34] D. Galindo, R. Roman, and J. Lopez, "A killer application for pairing: Authenticated key establishment in underwater wireless sensor networks," in *Proc. of the 7th International conference on Cryptogy and Network Security (CANS 2008)*, pp 120-132, 2008