Extending CertificateLess Authentication for Wireless Sensor Networks: A Novel Insight

Gaurav Sharma[1], Suman Bala[1] and Anil K. Verma[1]

[1] **Computer Science and Engineering, Thapar University, Patiala-147004, India**

Abstract

Authentication in low power devices is still considered to be an expensive process. CertificateLess Signature is one of the approaches to facilitate authentication in these devices. Wireless Sensor Networks (WSNs) are such low power inexpensive networks, which needs authentication of message. In this paper, a CertificateLess Signature proposed by Gong et al. is analyzed and an approach is being proposed to reduce the computation cost by more than 50 percent. The main benefits of our approach are (i) some computations can be performed by Key Generation Center (KGC) instead of sensor node (ii) signature size is merely increased a few bytes but saves a lot computation in multi-hop networks (iii) balance of computations on all sensor nodes and hence, increases the overall network lifetime.

Keywords: *Wireless Sensor Networks, Certificateless cryptography, Digital Signature.*

1. Introduction

Security is quite challenging in Wireless Sensor Networks (WSN) [1] because of their constrained nature in terms of resources such as limited memory, low processing power, limited bandwidth etc. Other constraints like, wireless communication medium, dense architecture and deployment in unattended and hostile areas make them prone to attack. Due to wireless communication in WSN, it attracts various adversaries to take advantage. As WSN is usually unattended deployed in hostile areas, adversary may have physical access and can obtain cryptographic materials stored in the sensor node. This prevents the direct use of existing security protocols designed for wired networks, to such environment [2]. For secure communication in WSN, the receiving node should communicate with a legitimate node so that the malicious node may not take advantage of this. Authentication is a crucial factor for WSN applications such as nuclear power plant where incorrect data may create serious problem. Moreover, providing authenticity is very difficult in WSN and there is a need of lightweight scheme in terms of less computation and communication cost [3,4].

The first solution to authentication problem can be thought of using traditional Public Key Cryptosystem (PKC) but WSN cannot bear the cost of implementing it. Several researchers tried to fit RSA and other variants into WSN but could not work out [5]. In 1984, Shamir et al. [6] proposed a novel revolutionary idea namely Identity Based Cryptosystem (IBC) which diminishes the cost of certificate management in PKC. In this approach, a publicly known string such as email id, name or social security number can be taken as public key by the user and the private key is generated by Private Key Generator (PKG), which is transmitted to the user via a secure channel. Earlier, the hardness assumption of the schemes was based on Factorization Problem (FP) or Discrete Logarithm Problem (DLP). Later, the paradigm is shifted to Elliptic Curve Discrete Logarithm Problem (ECDLP), based on elliptic curve cryptography. A lot number of Identity Based Signature schemes (IBS) found in literature is based on ECDLP. In IBC, the private key is generated by PKG, which increases the chances of impersonation attack by PKG. This problem is well known as key escrow problem. To eliminate this problem a novel concept was introduced by Riyami et al. [8] named as CertificateLess Public Key Cryptosystem (CL-PKC).

CL-PKC combines the advantages of PKC and IBC, eliminates the key escrow problem of IBC and removes the constraint of certificates, needed in PKC, for authentication of user's public key. In CL-PKC a trusted third party known as a Key Generation centre (KGC), computes partial private keys for users from their identities by using its global secret key and transmit it to the user via a secure channel. Unlike PKG in IBC, KGC does not have access to user's private keys. However, Riyami et al.'s [7] scheme was proved insecure against Type I adversary by Huang et al. [8]. Dozens of CertificateLess Signature (CLS) schemes based on DLP have been proposed and cryptanalysed [9,10,11,12,13]. Then, CLS schemes based on ECDLP has been proposed [14,15], which requires four pairing operations during verification algorithm, further improved in [16] to two bilinear pairing operations. However, the scheme [16] is found insecure in [17] against a key replacement attack.

Au et al. [18] suggested a new kind of malicious-but-passive-KGC attack where adversary may get access to the secret key of KGC and then they modified Hu et al.'s model [10] for performing an attack. Later, lots of short CLS schemes based on bilinear pairing have been proposed [19,20,21,22,23,24,25]. Xu et al. [26,27] proposed two CLS schemes for emergency mobile wireless cyber-physical systems and mobile wireless cyber-physical systems respectively, which was proven insecure [28] against public key replacement attack. Wang et al. [29] proposed a scheme, which need not to compute the pairing at the sign stage; rather it pre-computes and publishes as the system parameters. All the above certificateless signature (CLS) schemes discussed, are based on bilinear pairings.

The pairing operation is an expensive operation among other public key operations, such as elliptic curve point multiplication, elliptic curve point addition, etc. Some efficient CLS schemes have been designed that reduces the computational complexity of pairing operations. He et al. [30] developed an efficient short CLS scheme without pairing and proved insecure by [31] and [32] independently against strong type II adversary. Recently, Gong et al. [33] proposed a CLS scheme (we call it GL scheme throughout this paper) and claimed that [30] and [32] schemes are not exactly CLS. As GL scheme does not require pairing operation, we can use it for WSN. The signature takes only one point multiplication and verification takes four point multiplications. But this GL scheme will be very challenging to apply when receiver is a sensor node (not cluster head).

In this paper, a certificateless authentication approach for WSN has been proposed, which reduces the computation cost by more than 50 percent while, increasing the signature size to 20 bytes by reducing the burden of intermediary nodes using some modification in the existing scheme, hence increases the lifetime of the network. We modify the GL scheme to multi-hop network for WSN (we call it MGL scheme).

Roadmap: Section 2 describes the network infrastructure of WSN and need of authentication for WSN. In section 3 review of the Gong et al. [33] scheme followed by the modified version in section 4. The benefits of the proposed approach are being discussed in section 5 followed by the conclusion.

2. Network Infrastructures

Generally, WSN can either be homogeneous or heterogeneous. In most of the real time scenarios, to increase the lifetime of the network, heterogeneous network is preferred. In this paper, we consider a heterogeneous network with fixed number of cluster-heads. Further, there may be two types of network for the transmission of data. These are single-hop and multi-hop networks.

(i) Single-hop network: A network is said to be single-hop if the cluster-head is one hop away from the sensor node in a cluster. Figure 1 shows a single-hop network for WSN. In single-hop networks, it is easy for the cluster-head to aggregate the data and communicate it to the base-station only through other cluster-heads. In other words, the expensive verification is performed by the cluster-head itself. So, in the case of single-hop network, there is no need to modify the GL scheme.

(ii) Multi-hop network: A network is said to be multi-hop if multiple hops are needed to transfer data to the cluster-head. Figure 2 shows a multi-hop network for WSN. In multi-hop networks, if the next receiving node is not a cluster-head, then the task of receiving and aggregating data is very expensive for a sensor node. The sensor node has to authenticate the received data. The authentication can be provided by using signature schemes. Recently, Gong et al. [33] proposed a scheme, which can be considered as the most efficient and secure at this stage. The implementation of these schemes in sensor network is still at large.

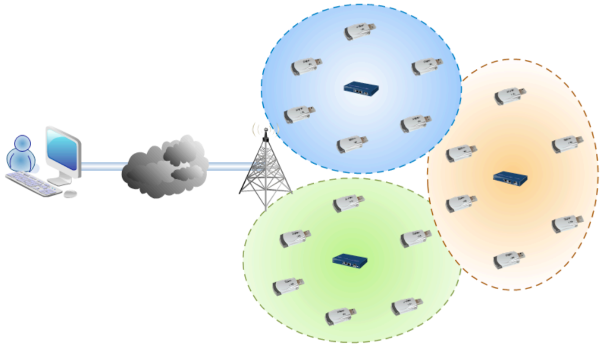

Fig. 1 Single-Hop Communication in Wireless Sensor Networks.

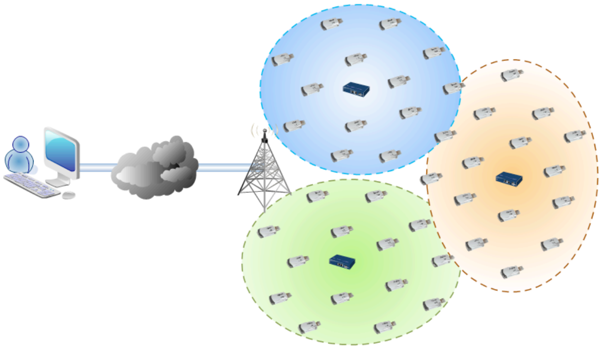

Fig. 2 Multi-Hop Communication in Wireless Sensor Networks.

The main target is to minimize the computation cost as well as with no or less affect on ciphertext size. If every node receives the sensed packet from the node below in the hierarchy, accumulates its own packet, the number of packets will increase continuously and will produce a heavy communication cost. But if each node has some aggregation criteria to aggregate the number of packets forwarded, cost can be reduced to a great extent. To perform the aggregation, authentication of message is important, especially for some critical applications like military, nuclear power plants etc.

3. Review of GL Short CLS Scheme

In this section, we briefly review the short certificateless signature scheme [33], which is based on ECDLP. The scheme works as follows:

Setup: For given k , KGC generates a cyclic additive group G of elliptic curve points with prime order q and generator of group be P . KGC chooses a random number $s\in Z_n^*$ and store it as master secret key $msk=s$. Then, it computes its master public key $P_{pub}=s\cdot P$. It chooses three secure one-way hash functions:
$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$, $H_2:\{0,1\}^*\times G\times G\times G\rightarrow Z_q^*$ and $H_3:\{0,1\}^*\times\{0,1\}^*\times G\times G\times G\rightarrow Z_q^*$.
The KGC then publishes public parameters
$param=\{G,P,P_{pub},H_1,H_2,H_3\}$ and keeps master secret key $msk=s$ secret.

Partial-Private-Key-Extract: For given $param$ and identity ID , KGC computes $R_{ID}=r_{ID}\cdot P$ and $h_{ID}=H_1(ID,R_{ID})$ for each signer with his/her identity $ID\in\{0,1\}^*$, where $r_{ID}\in Z_n^*$ is a random number. The KGC then computes $s_{ID}=r_{ID}+h_{ID}\cdot s$ mod n and sends $D_{ID}=(s_{ID},R_{ID})$ to the user via a secure channel. The D_{ID} is the partial private key of the user and user can confirm its validity by checking the following equation $s_{ID}\cdot P=R_{ID}+h_{ID}\cdot P_{pub}$. If the equation holds, the partial private key D_{ID} is valid; otherwise, the signer rejects the partial private key.

Set-Secret-Value: For given $param$ and identity ID , user chooses a random number $x_{ID}\in Z_n^*$ and sets it as his secret value.
Set-Private-Key: The signer uses $sk_{ID}=(x_{ID},s_{ID})$ as his private key.

Set-Public-Key: For given $param$, identity ID and secret value x_{ID} , user computes $pk_{ID}=x_{ID}\cdot P$ and set it as his public key.

Sign: For given $param$, identity ID , secret value x_{ID} , partial private key D_{ID} and a message m , user generates a signature $\sigma=(R_{ID},T_{ID},\tau_{ID})$ on chosen message m as follows:

(i) Chooses a random number $t_{ID}\in Z_n^*$ and computes $T_{ID}=t_{ID}\cdot P$
(ii) Computes $k_{ID}=H_2(ID,pk_{ID},R_{ID},P_{pub})$, $l_{ID}=H_3(m,T_{ID},ID,pk_{ID},R_{ID},P_{pub})$ and $\tau_{ID}=t_{ID}+l_{ID}\cdot(k_{ID}\cdot x_{ID}+s_{ID})$ mod n .
(iii) Computes $\sigma=(R_{ID},T_{ID},\tau_{ID})$ as a signature on message m .

Verify: For given $param$, identity ID , public key pk_{ID} , a signature $\sigma=(R_{ID},T_{ID},\tau_{ID})$ and a message m , the user verifies the validity of σ on message m as follows:

(i) Computes $h_{ID}=H_1(ID,R_{ID})$, $k_{ID}=H_2(ID,pk_{ID},R_{ID},P_{pub})$ and $l_{ID}=H_3(m,T_{ID},ID,pk_{ID},R_{ID},P_{pub})$.
(ii) Verify, $\tau_{ID}\cdot P=T_{ID}+l_{ID}\cdot(k_{ID}\cdot pk_{ID}+R_{ID}+h_{ID}\cdot P_{pub})$ holds.
(iii) If it is true, returns $\top$, else returns $\perp$.

4. Proposed Approach: MGL Short CLS Scheme

In this section, a modified approach to GL scheme has been presented, named as MGL, which works for multi-hop WSN. Setup, Set-Secret-Value, Set-Private-Key, Set-Public-Key algorithms works same as in GL scheme. Other algorithms work as follows:

Partial-Private-Key-Extract: For given $param$ and identity ID , KGC computes $R_{ID}=r_{ID}\cdot P$ and $h_{ID}=H_1(ID,R_{ID})$ for each signer with his/her identity $ID\in\{0,1\}^*$, where $r_{ID}\in Z_n^*$ is a random number. The KGC computes $s_{ID}=r_{ID}+h_{ID}\cdot s$ mod n and $h_{ID}\cdot P_{pub}$.

KGC then sends $D_{ID} = (s_{ID}, R_{ID})$ to the signer via a secure channel. It also sends $h_{ID} \cdot P_{pub}$ to signer and verifier both. The D_{ID} is the partial private key of the signer and signer can confirm its validity by checking the following equation $s_{ID} \cdot P = R_{ID} + h_{ID} \cdot P_{pub}$. If the equation holds, the partial private key D_{ID} is valid; otherwise, the signer rejects the partial private key.

Sign: For given $param$, identity ID, secret value x_{ID}, partial private key D_{ID} and a message m, signer generates a signature $\sigma = (R_{ID}, T_{ID}, \tau_{ID})$ on chosen message m as follows:

(i) Chooses a random number $t_{ID} \in Z_n^*$ and computes $T_{ID} = t_{ID} \cdot P$.

(ii) Computes $k_{ID} = H_2(ID, pk_{ID}, R_{ID}, P_{pub})$, $l_{ID} = H_3(m, T_{ID}, ID, pk_{ID}, R_{ID}, P_{pub})$ and $\tau_{ID} = t_{ID} + l_{ID} \cdot (k_{ID} \cdot x_{ID} + s_{ID}) \bmod n$. If the receiving node is a cluster head (powerful/full of resorces), then signer computes $\sigma = (R_{ID}, T_{ID}, \tau_{ID}, \infty)$ as a signature on message m. Otherwise, signer computes $\sigma = (R_{ID}, T_{ID}, \tau_{ID}, \tau_{ID} \cdot P)$ as a signature on message m.

Verify: For given $param$, identity ID, public key pk_{ID}, a signature $\sigma = (R_{ID}, T_{ID}, \tau_{ID}, \tau_{ID} \cdot P / \infty)$ and a message m, the user verifies the validity of σ on message m as follows:

(i) Computes $k_{ID} = H_2(ID, pk_{ID}, R_{ID}, P_{pub})$ and $l_{ID} = H_3(m, T_{ID}, ID, pk_{ID}, R_{ID}, P_{pub})$.

(ii) If $\tau_{ID} \cdot P$ is received then it can be directly used otherwise the verifier will perform this computation. Verify, $\tau_{ID} \cdot P = T_{ID} + l_{ID} \cdot (k_{ID} \cdot pk_{ID} + R_{ID} + h_{ID} \cdot P_{pub})$ holds.

(iii) If it is true, returns $\top$, else returns $\perp$.

5. Discussion

As WSN is a resource-constrained network, the main focus is to reduce the computation and communication cost. In the proposed approach, we modify the GL certificateless scheme [33] to reduce the overall computation in a multi-hop network. In the first modification, $h_{ID} \cdot P_{pub}$ will be computed by KGC instead of a sensor node, as this computation does not include any message information and private key. This can be easily communicated securely along with partial private key by KGC to the user. This will reduce the burden of both the users (signer and verifier) by one point multiplication. In the second modification, we introduced an extra field in the sign algorithm known as ∞, which is used to indicate whether this entry is already been computed or not. If the receiver is cluster-head, then the sender will not compute this new entry and forward it as ∞. But if receiver is normal sensor node, sender node will compute and send it to receiver so that receiver's burden can be reduced or shared.

Table 1: No. of Hops vs. Savings in Point Multiplications

Hop	*Scheme*	*Node1 (Signer)*	*Node2 (Signer & Verifier)*	*Node3 (Signer & Verifier)*	*Node4 (Signer & Verifier)*	*Node5 (Signer & Verifier)*	*Cluster-Head (Verifier)*	*T_{Mul} (Without CH)*	*Improvement* (%)
One	GL	$1^* + 1$					4	2	50
	MGL	1					3	1	
Two	GL	$1^* + 1$	$4 + 1^* + 1$				4	8	62.5
	MGL	2	2 + 1				3	5	
Three	GL	$1^* + 1$	$1^* + 1 + 4$	$1^* + 1 + 4$			4	14	64.2
	MGL	2	2 + 2	2 + 1			3	9	
Four	GL	$1^* + 1$	$1^* + 1 + 4$	$1^* + 1 + 4$	$1^* + 1 + 4$		4	20	65
	MGL	2	2 + 2	2 + 2	2 + 1		3	13	
Five	GL	$1^* + 1$	$1^* + 1 + 4$	$1^* + 1 + 4$	$1^* + 1 + 4$	$1^* + 1 + 4$	4	26	66.6
	MGL	2	2 + 2	2 + 2	2 + 2	2 + 1	3	17	

Note: * one point multiplication is performed by signer when Partial-Private-Key is received from KGC
GL: represents Gong et al. [33] scheme
MGL: represents modified approach for multi-hop infrastructure.

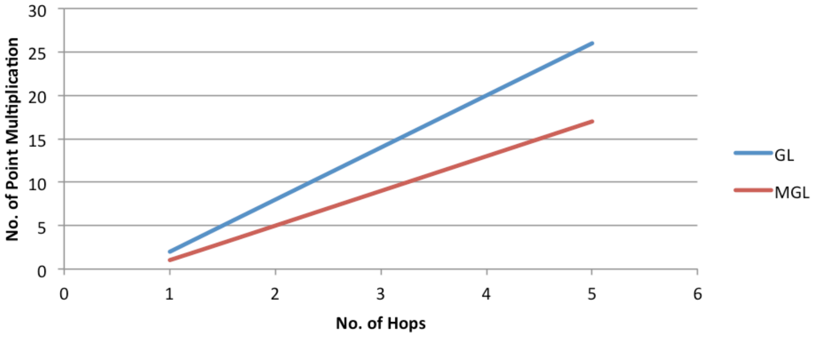

Fig. 3 Comparison of GL Scheme and Proposed Approach.

In our approach $\tau_{ID} \cdot P$ can be computed by sender, if the receiver is a normal sensor node. By this way, the sender can share the computation by two point multiplications in signature and two point multiplications in verification. But if the receiver node is cluster-head then the sender node will not compute this new entry and cluster head will compute it by itself. Further, if network is single-hop and GL scheme is considered, node 1 will perform two point multiplications (one in verification of partial private key, received from KGC and other in signature process) and cluster head will perform four point multiplications. In modified GL scheme, the only benefit is, $h_{ID} \cdot P_{pub}$ need not to be computed by sensor nodes, it will be provided by KGC.

Hence there is total saving of two point multiplications. If network is two-hop and GL scheme is considered, again node 1 need to perform two point multiplications, intermediate node will perform six point multiplication (four in verification, one in verification of partial private key, received from KGC and one in signature process) and cluster head will perform four point multiplications. But, in MGL scheme, only two point multiplications by node 1, three by intermediate node and three by cluster head. So, here total saving in point multiplication is three (without counting the cluster head computations). It can be easily predicted that in case of GL scheme, intermediate node will deplete its energy very quickly and hence, network lifetime will be less. Finally, in case of multi-hop network, MGL approach will make uniformity in point multiplications and as the number of hops increases, total savings in point multiplication will increase. After excluding cluster-head computations, the savings can be easily computed in multi-hop networks. Table I and figure 3 depicts the savings in point multiplications when GL scheme and proposed approach MGL is compared.

6. Conclusions

In most of the real time scenarios, the sensor network is not single-hop but it is multi-hop in nature. The proposed approach can be very efficiently utilized for resource constrained WSN nodes. The overall point multiplication has been reduced by more than 50 % in total.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless Sensor Networks: A Survey”, Computer Networks, Vol. 38, 2002, pp. 393-422.

[2] S. Olariu, “Information Assurance in Wireless Sensor Networks”, in 19th IEEE International Conference on Parallel and Distributed Processing Symposium, 2005.

[3] X. Chen, K. Makki, K. Yen and N. Pissinou, “Sensor Network Security: A Survey”, IEEE Communications Surveys and Tutorials, Vol. 11, No. 2, 2009, pp. 52-73.

[4] J. Walters, Z. Liang, W. Shi and V. Chaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid, and Pervasive Computing, 2006.

[5] A. Wander, N. Gura, H. Eberle, V. Gupta and S. Shantz, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, in 3rd IEEE International Conference on Pervasive Computing and Communications, 2005.

[6] A. Shamir, “Identity-Based Cryptosystems and Signature Schemes”, in CRYPTO'84 on Advances in Cryptology, 1984, pp. 47-53.

[7] S. Al-Riyami and K. Paterson, “Certificateless Public Key Cryptography”, in Asiacrypt'03, LNCS, Vol. 2894, 2003, pp. 452-473.

[8] X. Huang, W. Susilo, Y. Mu, F. Zhang, “On the security of certificateless signature schemes from asiacrypt 2003”, Cryptology and Network Security - LNCS, Vol. 3810, 2005, pp.13-25.

[9] H. Yum and P. Lee, “Generic construction of certificateless signature”, Information Security and Privacy - LNCS, Vol. 3108, 2004, pp. 200-211.

[10] B. Hu, D. Wong, Z. Zhang and X. Deng, “Key replacement attack against a generic construction of certificateless signature”, Information Security and Privacy - LNCS, Vol.

4058, 2006, pp. 235-246.

[11] B. Libert and J. Quisquater, "On Constructing Certificateless Cryptosystems from Identity Based Encryption", Public Key Cryptography – PKC'06 - LNCS, Vol. 3958, 2006, pp. 474-490.

[12] M. Gorantla and A. Saxena, "An efficient certificateless signature scheme", Computational Intelligence and Security - LNCS, Vol. 3802, 2005, pp. 110–116.

[13] X. Cao, K. Paterson and W. Kou, "An attack on a certificateless signature scheme", Cryptology ePrint Archive, Report 2006/367, 2006, http://eprint.iacr.org.

[14] X. Li, K. Chen and L. Sun, "Certificateless Signature and Proxy Signature Schemes from Bilinear Pairings", Lithuanian Mathematical Journal, Vol. 45, No. 1, 2005, pp. 76–83.

[15] Z. Zhang, D. Wong, J. Xu and D. Feng, "Certificateless public-key signature: security model and efficient construction", Applied Cryptography and Network Security - LNCS, Vol. 3989, 2006, pp. 293-308.

[16] W. Yap, S. Heng and B. Goi, "An Efficient Certificateless Signature Scheme", Emerging Directions in Embedded and Ubiquitous Computing - LNCS, Vol. 4097, 2006, pp. 322-331.

[17] J. Park and B. Kang, "Security analysis of the certificateless signature scheme proposed at Sec Ubiq 2006", Emerging Directions in Embedded and Ubiquitous Computing - LNCS, Vol. 4809, 2007, pp. 686-691.

[18] M. Au, J. Chen, J. Liu, Y. Mu, D. Wong and G. Yang, "Malicious KGC Attacks in Certificateless Cryptography", ACISP'07, LNCS, Vol. 4586, 2007, pp. 308–322.

[19] X. Huang, Y. Mu, W. Susilo, D. Wong and W. Wu, "Certificateless signature – revisited", Information Security and Privacy - LNCS, Vol. 4586, 2007, pp. 308-322.

[20] R. Tso, X. Yi and X. Huang, "Efficient and short certificateless signature", Cryptology and Network Security - LNCS, Vol. 5339, 2008, pp. 64–79.

[21] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings", Computer Standards and Interfaces, Vol. 31, No. 2, 2009, pp. 390–394.

[22] R. Tso, X. Yi and X. Huang, "Efficient and short certificateless signatures secure against realistic adversaries", Journal of Supercomputing, Vol. 55, No. 2, 2011, pp. 173–191.

[23] C. Fan, R. Hsu and P. Ho, "Truly Non-Repudiation Certificateless Short Signature Scheme from Bilinear Pairings", Journal of Information Science and Engineering, Vol. 27, No. 3, 2011, 969-982.

[24] K. Choi, J. Park and D. Lee, "A new provably secure certificateless short signature scheme", Computers and Mathematics with Applications, Vol. 61, No. 7, 2011, pp. 1760–1768.

[25] R. Tso, X. Huang and W. Susilo, "Strongly secure certificateless short signatures", The Journal of Systems and Softwares, Vol. 85, No. 6, 2012, pp. 1409–1417.

[26] Z. Xu, X. Liu, G. Zhang and W. He, "McCLS: Certificateless Signature Scheme for Emergency Mobile Wireless Cyber-Physical Systems", International Journal of Computers, Communications & Control, Vol. 3, No. 4, 2008, pp. 395-411.

[27] Z. Xu, X. Liu, G. Zhang, W. He, G. Dai and W. Shu, "A Certificateless Signature Scheme for Mobile Wireless Cyber-Physical Systems", in IEEE 28th International Conference on Distributed Computing Systems Workshops, ICDCS '08, 2008, pp. 489-494.

[28] F. Zhang, S. Li, S. Miao, Y. Mu, W. Susilo and X. Huang, "Cryptanalysis on two certificateless signature schemes", International Journal of Computers, Communications & Control, Vol. 5, No. 4, 2010, pp. 586-591.

[29] C. Wang, D. Long and Y. Tang, "An Efficient Certificateless Signature from Pairings", International Journal of Network Security, Journal of Information Science and Engineering, Vol. 8, No. 1, 2009, pp. 99-100.

[30] D. He, J. Chen and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings", International Journal of Communication Systems, 2011.

[31] M. Tian and L. Huang, "Cryptanalysis of a certificateless signature scheme without pairings", International Journal of Communications Systems, 2012.

[32] J. Tsai, N. Lo and T. Wu, "Weaknesses and improvements of an efficient certificateless signature scheme without using bilinear pairings", International Journal of Communications Systems, 2012.

[33] P. Gong and P. Li, "Further improvement of a certificateless signature scheme without pairing", International Journal of Communications Systems, 2012.

Gaurav Sharma received his M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. He had received M. Sc. as well as B. Sc. degree from CCS University, Meerut, India. He is pursuing Ph.D from Thapar University, Patiala, India. He has published over 20 papers in referred journals and conferences (India and Abroad). He is member of various program committees for different International/National Conferences and is on the review board of various journals. He is a member of IEEE. His research interests include wireless sensor networks, cryptography.

Suman Bala received her M.E degree in Computer Science & Engineering from Thapar University, Patiala, India. She had received B.Tech degree from Punjab Technical University, Jalandhar, India. She is pursuing Ph.D from Thapar University, Patiala, India. She has published over 20 papers in referred journals and conferences (India and Abroad). She is member of various program committees for different International/National Conferences and is on the review board of various journals. She is a member of ACM. Her research interests include wireless sensor networks, cryptography and key management.

Anil K. Verma is currently working as Associate Professor in the department of Computer Science and Engineering at Thapar University, Patiala in Punjab (INDIA). He received his B.S. and M.S. in 1991 and 2001 respectively, majoring in Computer Science and Engineering. He has worked as Lecturer at M.M.M. Engg. College, Gorakhpur from 1991 to 1996. From 1996 he is associated with the same University. He has been a visiting faculty to many institutions. He has published over 80 papers in referred journals and conferences (India and Abroad). He is member of various program committees for different International/National Conferences and is on the review board of various journals. He is a senior member (ACM), LMCSI (Mumbai), GMAIMA (New Delhi). He is a certified software quality auditor by MoCIT, Govt. of India. His main areas of interests are: Programming Languages, Soft Computing, Bioinformatics and Computer Networks. His research interests include wireless networks, routing algorithms and securing ad hoc networks.