Hybrid Key Management Technique for WSN's

Ravi Kishore Kodali and Sushant Chougule

Department of Electronics and Communications Engineering
National Institute of Technology, Warangal
Warangal, 506004 Andhra Pradesh, India

Abstract. Wireless sensor networks are envisaged in military, commercial and healthcare applications, where data security is an important aspect. Security of the data in the network is based on the cryptographic technique and the way in which encryption and decryption keys are established among the nodes. Managing the keys in the network includes node authentication, key agreement and key update phases which poses an additional overhead on network resources. Both Symmetric and Asymmetric key techniques when applied separately in WSN fails to provide a scheme suitable for wide range of applications. Hybrid key management scheme is scalable alternative to match security requirements of WSN with minimum overhead on available resources. Heterogeneous WSN is considered in which ID based key establishment and polynomial based key pre-distribution scheme are proposed for higher and lower level of hierarchy respectively. The results of the proposed hybrid key management scheme indicate reduced resource overhead and improved security level.

Keywords: WSN, Elliptic curves, symmetric key pre-distribution, IBC.

1 Introduction

Wireless sensor networks (WSN's) are being used in wide range of military and commercial applications. A WSN consists of tiny resource constrained sensor nodes and special monitoring device termed as base station. Sensor nodes act as the skin, which collect the data from surrounding environment and forward to the base station, the brain of the network, controls the data flow. WSN technology is expected to play crucial role in near future as the means of global data communication. 'Internet of things'[1] idea, proposed recently, considers WSN as the basic element to gather data. The collected data is then made globally available by connecting many small WSNs to the Internet. In such scenario, information collected by WSN's would have transcended value compared to its previous small scale application. Consequently, security of the data also plays a vital role.

Confidentiality, Integrity and Authenticity of the data collected are the main issues in sensor network security. Wireless nature of the network along with the lack of computational ability of sensor nodes poses many challenges in the implementation of security protocol for WSN. RSA-1024 and AES cryptographic

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 854–865, 2013.

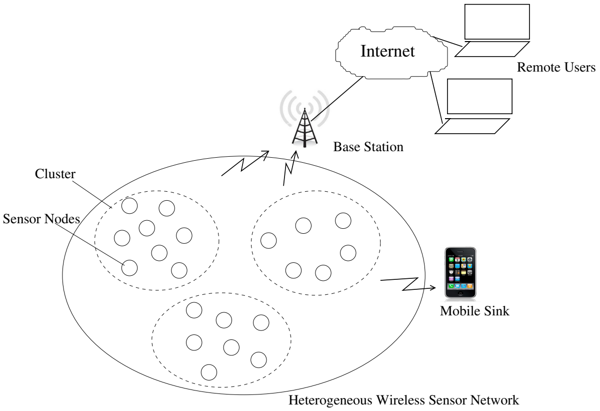

Fig. 1. Wireless Sensor network scenario

standards are widely used in secure internet transactions[2]. But computational cost of these schemes is not feasible over sensor nodes. Elliptic curve cryptography is proved to be the most suitable asymmetric key technique for WSN because of small key size$(160-bit)$ with equivalent security[3]. Effective applicability of these cryptographic schemes in the network depends on the key management technique used.

Key Management technique is the backbone of any network security scheme. Secured channel for data transmission in a WSN is provided by key establishment protocol. The design of key management protocol mainly focusses on the consumption of resources like memory, energy and processing time by the scheme, resilience against various attacks, communication overhead and scalability. At the system level, the demands from key management technique being resilience against node capture, forward secrecy, backward secrecy, node revocation on intrusion detection and security against network level attacks. Both symmetric and asymmetric key techniques used for computer networks fail to satisfy these WSN specific security requirements.

In this paper, a hybrid key management technique is proposed for heterogeneous wireless sensor network. First, clusters are formed based on the location of WSN nodes. A suitable cluster head selection algorithm can be used to elect and update the cluster head. A cluster head is assumed to have the same hardware resources as those of other nodes. The base station communicates with a cluster head and establishes secure connection using Identity Based Cryptography (IBC). All the cluster heads are securely connected using IBC, which is more secure due to the elliptic curve discrete logarithmic problem $(ECDLP)$. Nodes inside a cluster use polynomial based pairwise key pre-distribution scheme and avoid extra computational burden. Section II discusses the related work in the field of WSN key management. Section III provides mathematical background for IBC and Section IV presents the proposed hybrid key management scheme.

2 Related Work

Key management techniques proposed for WSN attempt to seek perfect connectivity and resilience against node capture attack[4]. This means that each node should be able to communicate with every other node in the network and if a node gets captured, secured connections of other nodes should remain intact. The simplest way to establish key management in a WSN is to make use of single master key for the entire network. It provides full connectivity and scalability, but a single node compromise can expose the whole network. To circumvent this problem, pairwise keys can be pre-distributed in each node so that capturing of a node will affect only single node keeping all the other connections secure. But for a WSN, consisting N nodes, each node needs to store (N-1) pairwise keys to achieve full connectivity. Apart from stringent memory requirements, this technique limits the scalability of the WSN.

To provide a trade-off between connectivity and resilience against node capture attack, Eschenauer and Gligor[4] first proposed probabilistic key pre-distribution scheme. In this scheme, prior to deployment, a subset of the keys from a large key pool is stored in each node. Each key is tagged with unique identifier. Nodes broadcast key identifiers to their neighbours and pairwise key with the nodes having at least one common key. Nodes that are unable to establish a direct pairwise key, enters into secure path discovery phase. The node capture attack affects non-captured nodes as captured node contains common keys with a given probability.

Improvement to this scheme is Q-composite random key distribution[5], which requires nodes to contain at least Q common keys to establish pairwise key. This technique reduces the probability of compromising secured link between non captured nodes by the factor Q. Another improved random key pre-distribution uses hash function H[6]. For node i key from key pool is hashed $(i-1)$ times. For establishing pairwise key between nodes A and B having keys $K_A = H^{i_a}\left(K_i\right)$ and $K_B = H^{i_b}\left(K_i\right)$ respectively shares i_a and i_b value. If $i_a < i_b$ node B can easily calculate symmetric key as

$$K_{AB} = H^{i_a - i_b}\left(K_B\right) \tag{1}$$

Polynomial based pair wise key distribution scheme[7] provides more resilience against node capture attack with less memory requirement. Polynomial $p\left(x,y\right)$ of degree t and having coefficients over $GF\left(q\right)$ is used to establish keys between the nodes. The polynomial has the property $p\left(x,y\right) = p\left(y,x\right)$

$$p\left(x,y\right) = \sum_{0 \leq i,j \leq t}^{t} a_{ij} x^i y^j , \tag{2}$$

where a_{ij} are the elements of symmetric matrix A of order $t \times t$. Node with identity i stores $p\left(i,y\right)$ and to establish pair wise key with the node having identity j calculates stored polynomial over point j, $k_{i,j}$. Similarly node j computes pair wise key $p\left(j,y\right)$ over point i, $k_{j,i}$. Because of symmetry property of A, $k_{i,j} = k_{j,i}$.

Matrix A is the secret information in the network and $(t+1)/2$ nodes has to compromised to calculate A.

Improvement in key pre-distribution scheme can be obtained by combination of probabilistic key pre-distribution, Q-composite key generation and Polynomial pool based key pre-distribution scheme[8]. Proposed schemes have threshold property which means that network security is maintained if number of nodes captured is less than some threshold. Comparing communication overhead, memory requirement, connectivity and security aspects improvement achieved by combination of different schemes is highlighted.

Key pre-distribution schemes are based on security vs connectivity tradeoff. Hence to achieve both security and connectivity with minimum resource overhead many researchers have focussed on asymmetric key establishment techniques suitable for Wireless sensor networks. Public key infrastructures(PKI)[2] used in computer networks requires Certification authority(CA) to bind the public key of user to its identity. Mechanism to handle large certificates and computationally intensive Digital Signature algorithms are too complex to implement on resource constrained WSN.

Shamir[9] first introduced Identity based encryption scheme which uses unique ID of the device as its public key. For computer networks, this ID can be email address or IP address. In the context of WSN, ID can be assigned by network deploying party to ensure its uniqueness. Identity based key management scheme does not require CA but another entity termed as Private key generator (PKG) is used to generate private keys from node's ID. Research on ID based key techniques for WSN focus on Pairing based cryptography (PBC) to establish pairwise key between the sensor nodes. ID-based key management scheme is implemented in MANET with key refreshment technique[10]. Apart from *Setup*, *Extract*, *Encrypt* and *Decrypt* phases in IBE, $Refresh$ phase is added to update private keys after certain amount of time. This achieves Forward secrecy and dynamic key management. Taking this work further, $Refresh$, *Recover* and *Revocation* phases are added in ID-based key management technique for WSN[11]. In their scheme more than one base stations are used to generate private key. In effect, this scheme achieves forward secrecy, backward secrecy, intrusion detection and resilience against base station capture attack. To achieve dynamic network topology cluster formation and group key management techniques are used along with key update and Revocation mechanism[12].

WSN nodes are energy constrained devices. The need of pairing algorithm and its implementation on ARM processor is studied[13] using Pairing functions from MIRACL[14] library. Pairing is considered as the most power consuming operation. Its results show that $0.444J$ power is consumed by the pairing algorithm alone. Energy consumption and execution time of point operations over super singular elliptic curve are also presented. TinyPBC[15] is another pairing algorithm for ID-based Non-Interactive Key distribution in WSN's. It demonstrates how sensor nodes can exchange keys in authenticated and non-interactive way. Paper shows that MICA2 sensor nodes with ATmega128L micro-controller $(8-bit/7.3828MHz)$ computes pairings in $5.5s$ time. K. McCusker [16] presented symmetric key distribution scheme based on Identity based cryptography

(IBC). The idea is to use asymmetric key algorithm (IBC) for authenticated key agreement and then encryption can be performed using symmetric keys generated. An accelerator hardware for Tate pairing achieves running time of $1.75ms$ and energy consumption of $0.08mJ$. These are the best result in the field of ID-based key management scheme for WSN.

3 Mathematical Background

Concept of ID-based cryptography relies on the fact that device in the network can be uniquely identified by ID assigned to it. To calculate pairwise key using ID of the device pairing based cryptography can be used. It should be noted that Identity based cryptography can be implemented in WSN only after making use of bilinear pairing properties.

Bilinear Pairing: Let G be an additive cyclic group of order n and let G_T be the multiplicative group. bilinear pairing is a computable, non-degenerate mapping function,

$$e : G \times G \to G_T$$

Bilinearity property: $\forall P, Q \in G$, and $\forall a, b \in Z*$

$$e\left([a]\,P, [b]\,Q\right) = e\left([a]\,P, Q\right)^b = e\left(P, [b]\,Q\right)^a = e\left(P, Q\right)^{ab}$$

3.1 Weil Pairing

Weil pairing maps points on elliptic curve over $GF\left(q\right)$ to the root of unity in extension field $GF\left(q^k\right)$. This implication transforms Elliptic curve discrete logarithmic problem $(ECDLP)$ in $GF\left(q\right)$ to discrete logarithmic problem (DLP) in $GF\left(q^k\right)$. Let E: Elliptic curve over prime field GF_q, Point $P, Q \in r-$torsion group. Weil pairing mapping function can be computed as

$$e\left(P, Q\right) = \frac{f_P\left(A_Q\right)}{f_Q\left(A_P\right)}$$

To calculate Weil Pairing mapping function Miller's algorithm is used twice. Following Explicit formulas are used in Miller Algorithm[3] $E : y^2 = x^3 + ax + b$
$P_1, P_2 \in E$, $P_1 = (x_1, y_1)$ and $P_2 = (x_1, y_1)$
Let $P_3 = P_1 + P2$
For $x_1 = x_2, y_1 = -y_2$,

$$V : X - x_1 = 0 \tag{3}$$

For $P_1 = P_2$ Slope is

$$\lambda_1 = \frac{3x_1^2 + a}{2y_1} \tag{4}$$

Tangent line is

$$T : Y - (\lambda_1 X + y_1 - \lambda_1 x_1) = 0 \tag{5}$$

Algorithm 1. Miller Algorithm for Weil Pairing

```
$f_1 \leftarrow V_{P+R}(Q)/L_{P,R}(Q)$
$f \leftarrow f_1$
$Z \leftarrow P$
for $i \leftarrow t-1$ to 0 do
    $f \leftarrow f^2 T_Z(Q)/V_{2Z}(Q)$
    $Z \leftarrow 2Z$
    if $r_i = 1$ then
        $f \leftarrow f * f_1 * V_{P+R}(Q)/L_{P,R}(Q)$
        $Z \leftarrow Z + P$
    end if
end for
```

For $P_1 \neq P_2$, slope is

$$\lambda_2 = \frac{y_2 - y_1}{x_2 - x_1} \tag{6}$$

Line equation is

$$L : Y - (\lambda_2 X + y_1 - \lambda_2 x_1) = 0 \tag{7}$$

3.2 Tate Pairing

Weil pairing using Miller algorithm is not suitable for resource constrained hardware platforms. Instead Tate pairing over super singular elliptic curves in binary field can be used to implement pairing. η_T algorithm[17] computes Tate pairing over super singular curve $E(GF(2^m)) : y^2 + y = x^3 + x + b$.

Algorithm 2. η_T Algorithm

```
Input:$P, Q$
Output:$e(P, Q)$
Let $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$
$f \leftarrow 1$
for i$\leftarrow$ 1 to $m$ do
    $u \leftarrow x_p^2$
    $g \leftarrow (u+1).(x_P + x_Q) + u + y_P + y_Q + (u + x_Q + 1)s + t$
    $f \leftarrow f.g$
    $x_P \leftarrow u, y_P \leftarrow y_P^2, x_Q \leftarrow \sqrt{x_Q}, y_Q \leftarrow \sqrt{y_Q}$
end for
return $f^{q^2-1}$
```

3.3 Pairwise Key Establishment

Pairwise key generation between two nodes A, B can be verified using bi-linearity property as follows:
Let K_i : Private key of node i,

ID_i: Identity of node i,
e : bilinear mapping function,
K_{ij}: pair wise key for nodes i
j, H: Hash function,
s: Master secret key

$$K_{AB} = e(K_A, H(ID_B))$$
$$K_{AB} = e(s.H(ID_A), H(ID_B))$$
$$K_{AB} = e(H(ID_A), s.H(ID_B))$$
$$K_{AB} = e(K_B, H(ID_A))$$
$$K_{AB} = K_{BA}. \tag{8}$$

4 Scheme

The scheme proposes hybrid key management technique formed by the combination of symmetric and asymmetric key primitives. The main aim of the scheme is to achieve maximum secured connectivity and minimize energy and memory overhead over the entire network. Distributing the computational load among the different nodes, overall performance of the network, in terms of security, energy usage and connectivity, can be improved. We consider that all same nodes are similar with respect to their energy, memory and computational resources. Base station (BS) is assumed to have more computational power. Network architecture is heterogeneous. Network is clustered after the deployment and cluster head (CH) is selected by the base station. Identity based key management scheme is used to establish secure connection among different cluster heads and between base station and cluster head. This key establishment is dynamic and done on-line. Sensor nodes inside the cluster are securely connected by making use of polynomial based key pre-distribution primitives. Following subsections describes detailed implementation of the scheme.

4.1 Setup

Before deployment of the network cryptographic primitives need to be stored in sensor nodes and base station to establish keys in the network.

- $ID_i \leftarrow$ ID of the node i stored by deploying authority
- $e \leftarrow$ Tate pairing function over binary field $GF\,(2^m)$
- $s \leftarrow$ Master key stored in BS
- $p(i, y) \leftarrow$ bivariate polynomial calculated using symmetric matrix M, stored in node i
- $H \leftarrow$ Hash function stored in each node to map Identity of node to point on elliptic curve
- $E \leftarrow$ Elliptic curve parameters

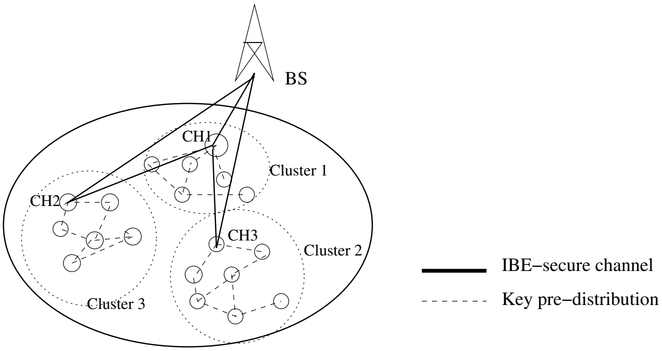

Fig. 2. Hybrid Key establishment scheme for WSN

Hash function H is nothing but Koblitz encoding method on elliptic curve[3].It is assumed that sensor nodes are deployed randomly on the field and nodes are not tamper resistant. Instead of high cost tamper resistant nodes, nodes are replaced when they found to be captured. To avoid the replay attack in the network, Time Stamp(TS) is concatenated to each message.

4.2 Secure Cluster Formation

After deployment base station selects the cluster head one by one. Number of cluster heads to be formed is programmed into base station. First cluster head is randomly selected. Following communication takes place:

$$BS \rightarrow CH_i : s.ID_{BS}\text{:Public key of BS}$$

$s.ID$ multiplication takes place over elliptic curve, hence to deduce s is computationally exhaustive task by the implication of $ECDLP$.Cluster head calculates pairwise key as follows:

$$K_{CH_i,BS} = e(s.ID_{BS}, ID_{CH_i}) \tag{9}$$

At the same time BS can also calculate pairwise key using bilinear pairing property:

$$K_{BS,CH_i} = e(s.ID_{CH_i}, ID_{BS}) \tag{10}$$

Selected cluster head sends *Hello* packet to its neighbour nodes and adds the nodes to its group upon response from them. Group list, encrypted using pairwise key calculated previously, is sent to BS. BS station stores the list and selects next cluster head which is not present in the stored list. In this way all clusters are formed in secured way.

4.3 Key Agreement Phase

Case 1: I two nodes inside the same cluster want to establish pairwise key, bivariate polynomial $p(x, y)$, given by equation (2) stored in the node is used.

For example node i and j are in same cluster. Pairwise key k_{ij} calculated as,

$$k_{ij} = p(i,y).M.p(j,y)' \tag{11}$$

Similarly, node j calculates k_{ji} and by the symmetry property of bivariate polynomial,

$$k_{ij} = k_{ji} \tag{12}$$

Case 2: When one cluster head wants to communicate with another cluster head, it request pairwise key to the base station. In this case BS act as PKG and send pairwise key to both the cluster heads through previously established secure channel. *Case 3:* If node in one cluster wants to communicate to the node in another cluster, three step key agreement is performed. First pairwise key between cluster head and node is established using bivariate polynomial. In the next step, using ID based key encryption two cluster heads are securely connected. In the last step again pairwise key between cluster head and destination node is established.

4.4 Key Update

Cluster heads are changed periodically. New cluster head is decided by the nodes in cluster depending upon the pre-defined threshold level of energy. Newly elected cluster head publish its ID to BS. BS and new cluster head generates fresh pairwise key using Tate pairing function given by Algorithm [2]. Also base station broadcast new cluster head ID to other cluster heads. Key update mechanism also suits the energy constraints of the nodes. Single node energy is avoided and at the same time key refreshment is also achieved.

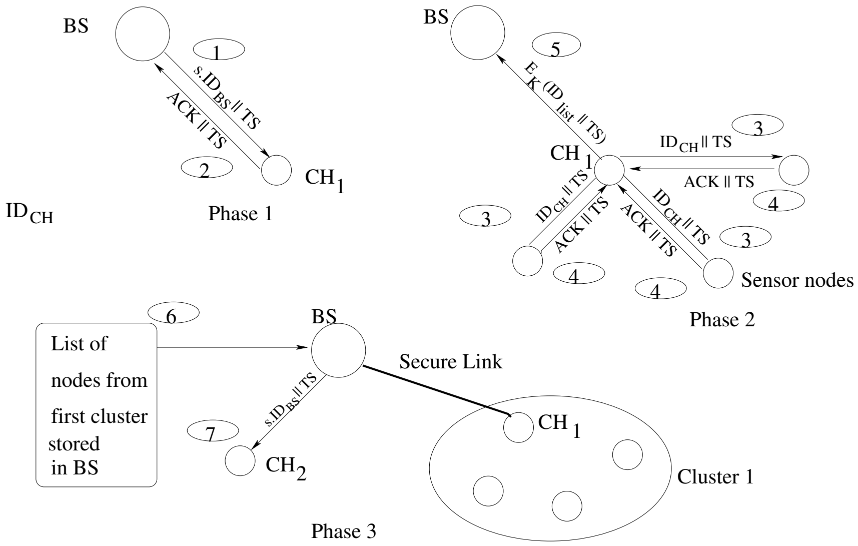

Fig. 3. Key establishment phases

4.5 Revocation

BS manages the list of authenticated cluster heads while cluster head holds the list of authenticated nodes in the cluster. As soon as number of nodes captured in cluster goes above certain threshold, cluster head reports security threat to the BS and that cluster is removed from authenticated cluster heads list. As nodes are less in cost new nodes are installed instead of using costly tamper resistant nodes.

5 Results and Discussion

Hybrid key management technique provides scalable security option for large wireless sensor networks. ID-based key technique provides secured connection at the cost of high computational requirement. Comparison of hybrid key scheme and ID-based key scheme[18] with respect to algorithm execution time and energy consumption. Instead of considering resource consumption by single node resources consumed throughout the network are analysed. For time calculation worst case scenario, in which all keys are established different times, is assumed.
Number of nodes: 500
Number of clusters: 20
Numner of nodes in cluster: 25

Table 1. Comparison with ID-based key scheme

Key Management scheme	Timing	Energy
IBK scheme (using Tate pairing)	1330s	31.365J
Hybrid key scheme	53.2s	1.255J

Different key management related issues of the proposed hybrid key technique are discussed as follows.
Scalability: Cluster head formation mechanism adopted in the scheme allows large sensor nodes to be deployed with minimum overhead on the memory and energy resources. Cluster head formation mechanism is secure and new clusters can be easily added without causing any threat to security to expand the network.
Forward and backward secrecy: Because of periodic key update, new nodes can not detect previous messages. Revocation phase take care that old nodes in the network should not be able to read new messages in the network. *Communication overhead:* Non interactive key establishment using ID based cryptography minimizes communication overhead.
Memory overhead: As polynomial pool based key technique is used at cluster level less number of polynomial coefficients are need to be stored. If m cluster are formed for n number of nodes, memory overhead is reduced by factor $\frac{m}{n}$

Energy consumption: Cluster head consumes most of the energy and there is a chance of single node energy drain out. Energy consumption is distributed among all the nodes as cluster head is update periodically. Most of the node expect cluster heads uses polynomial based key technique which requires less energy compared to IBE. Also energy is conserved by avoiding communication between cluster heads.

6 Conclusion

Key management technique designed by combination of symmetric and asymmetric key primitives over different levels of hierarchy proves to be an effective solution for resource constrained networks. Security of the overall network is improved compared to polynomial based key pre-distribution scheme with minimized memory overhead. At the same time, energy consumption due to computationally intensive IBK scheme is limited to the nodes in higher level of hierarchy. Also, Cluster head rotation policy avoids energy drain of single node and distribute energy overhead among different nodes. Energy consumption and execution time results calculated for the proposed schemes shows that considerable amount of energy and time overhead can be reduced by the application hybrid key management scheme.

References

1. Atzori, L., Iera, A., Morabito, G.: The internet of things: A survey. Computer Networks 54(15), 2787–2805 (2010)
2. William, S., et al.: Cryptography and Network Security, 4/e. Pearson Education India (2006)
3. Hankerson, D., Menezes, A., Vanstone, S.: Guide to elliptic curve cryptography. Springer (2004)
4. Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41–47. ACM (2002)
5. Chan, H., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proceedings of 2003 Symposium on Security and Privacy, pp. 197–213. IEEE (2003)
6. Shan, T., Liu, C.: Enhancing the key pre-distribution scheme on wireless sensor networks. In: IEEE Asia-Pacific Services Computing Conference, APSCC 2008, pp. 1127–1131. IEEE (2008)
7. Blom, R.: An optimal class of symmetric key generation systems. In: Beth, T., Cot, N., Ingemarsson, I. (eds.) EUROCRYPT 1984. LNCS, vol. 209, pp. 335–338. Springer, Heidelberg (1985)
8. Rasheed, A., Mahapatra, R.: Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks. IEEE Transactions on Parallel and Distributed Systems 22(1), 176–184 (2011)
9. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)

10. Balfe, S., Boklan, K.D., Klagsbrun, Z., Paterson, K.G.: Key refreshing in identity-based cryptography and its applications in manets. In: IEEE Military Communications Conference, MILCOM 2007, pp. 1–8. IEEE (2007)
11. Saab, S., Kayssi, A., Chehab, A.: A decentralized energy-aware key management scheme for wireless sensor networks. In: 2011 International Conference for Internet Technology and Secured Transactions (ICITST), pp. 504–508. IEEE (2011)
12. Jian-wei, J., Jian-hui, L.: Research on key management scheme for wsn based on elliptic curve cryptosystem. In: First International Conference on Networked Digital Technologies, NDT 2009, pp. 536–540. IEEE (2009)
13. Doyle, B., Bell, S., Smeaton, A., Mccusker, K., O'Connor, N.: Security considerations and key negotiation techniques for power constrained sensor networks. The Computer Journal 49(4), 443–453 (2006)
14. Scott, M.: Miracl–multiprecision integer and rational arithmetic c/c++ library. Shamus Software Ltd., Dublin, Ireland (2003), http://www.shamus.ie
15. Oliveira, L., Scott, M., Lopez, J., Dahab, R.: Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks. In: 5th International Conference on Networked Sensing Systems, INSS 2008, pp. 173–180 (June 2008)
16. McCusker, K., O'Connor, N.E.: Low-energy symmetric key distribution in wireless sensor networks. IEEE Transactions on Dependable and Secure Computing 8(3), 363–376 (2011)
17. Barreto, P., Galbraith, S., hÉigeartaigh, C., Scott, M.: Efficient pairing computation on supersingular abelian varieties. Designs, Codes and Cryptography 42(3), 239–271 (2007)
18. Szczechowiak, P., Kargl, A., Scott, M., Collier, M.: On the application of pairing based cryptography to wireless sensor networks. In: Proceedings of the Second ACM Conference on Wireless Network Security, pp. 1–12. ACM (2009)