Key Management Technique for WSNs

Ravi Kishore Kodali
Department of Electronics and Communication Engineering,
National Institute of Technology, Warangal
Andhra Pradesh, 506004, India

***Abstract*—In Wireless sensor networks (WSNs), many tiny sensor nodes communicate using wireless links and collaborate with each other. The data collected by each of the nodes is communicated towards the gateway node after carrying out aggregation of the data by different nodes. It is necessary to secure the data collected by the WSN nodes while they communicate among themselves using multi hop wireless links. To meet this objective it is required to make use of energy efficient cryptographic algorithms so that the same can be ported over the resource constrained nodes. It is needed to create trust initially among the WSN nodes while using any of the cryptographic algorithms. Towards this, a key management technique needs to be made use of. Due to the resource constrained nature of the WSN nodes and the remote deployment of the nodes, an implementation of conventional key management techniques is infeasible. This work proposes a key management technique, with its reduced resource overheads, which is highly suited to be used in hierarchical WSN applications. Both Identity based key management (IBK) and probabilistic key pre-distribution schemes are made use of at different hierarchical levels. The proposed key management technique has been implemented using IRIS WSN nodes. A comparison of resource overheads has also been carried out.**

Keywords: WSN, security, Key management, IBK

I. Introduction

Wireless sensor networks (WSNs) are being widely used to monitor various events and to track objects in remote and hazardous areas. In majority of the out door WSN applications the nodes are deployed randomly and then the nodes organize themselves into a network autonomously. Any node deletion or addition to this network does not require any human intervention [1],[2]. The WSN nodes have constrained resources: limited memory, less compute power, short radio range and finite battery energy. When such nodes are deployed randomly in the field, it may not be possible or feasible to be able to replace the batteries of the nodes. Hence, the lifetime of a node is primarily dependent on the usage of the limited energy and its conservation during the network operation. It is essential for the protocols being used to conserve energy by reducing computational and communication overheads so as to extend the network lifetime.

One of the primary duties of a sensor node is to gather data from its surroundings. In WSNs the nodes are arranged using either a flat topology or hierarchical topology. The flat topology based networks are usually small in size and normally used in indoor applications, where structured deployment is feasible. In order to extend the network lifetime, a hierarchical topology becomes the natural choice. In this the sensor nodes are divided into many groups or clusters and a group leader or a cluster head is elected for every cluster. A cluster head (CH) aggregates the data received from its constituent nodes and forwards the same towards the base station (BS) either directly or using multi hop wireless communication path. The BS monitors the data flow in the network. Any authorised user can gain access to the data collected by the WSN through the BS. Figure 1 shows a WSN with Internet connectivity.

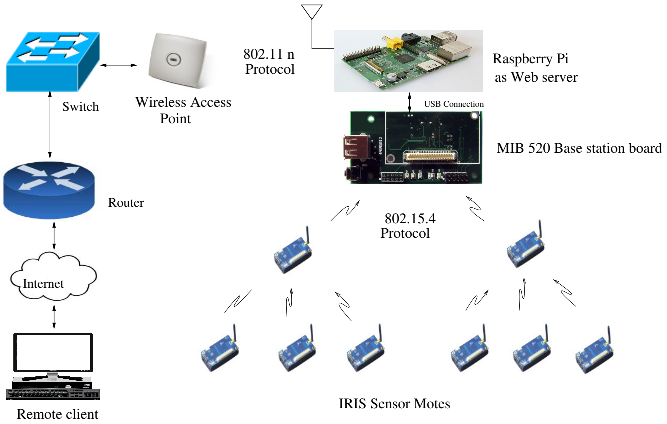

Fig. 1. Hierarchical Wireless sensor network scenario

The nodes are arranged in an hierarchical manner and the leaf nodes communicate with the BS through their respective CHs. To achieve flexibility in the deployment, the homogeneous sensor nodes are used and cluster heads are selected after the deployment. The BS is connected to a portable computer board, *Raspberry Pi* [3], which eliminates the need of a PC at the BS and further enhances the deployment flexibility. Hence, network security is inevitable in WSNs to make them more reliable.

While evolving a security model for WSNs various cryptographic techniques are used. These techniques heavily rely on creation of initial trust among the nodes. Key management is one of the most important techniques. This work proposes a key management technique for hierarchical WSNs. The CHs are connected using more secure but resource consuming Identity based key (IBK) management technique, whereas for the leaf nodes the probabilistic key pre-distribution technique is used. The proposed hybrid key management technique is discussed and the results of the WSN implementation are given. Section II discusses previously proposed key management schemes for WSNs. Section III discusses the proposed scheme and section IV gives its implementation details. Section V presents the analysis of the scheme based on security parameters and resource overhead and section VI concludes the paper with remarks on the proposed scheme.

978-1-4799-2027-3/14/$31.00 ©2014 IEEE

II. Literature Review

Both symmetric and asymmetric key management techniques for WSNs are proposed in the literature. Earlier, researchers were more focussed on symmetric key pre-distribution schemes which are easy to implement [4]. A probabilistic key pre-distribution scheme [5] provided a trade-off between connectivity and resilience against node capture attack. A subset of keys from a large key pool is stored in each of the nodes prior to node deployment in this scheme. Each key is assigned with a unique key identifier. Each node broadcasts its key identifiers to its neighbours and a pairwise key with every node having at least one common key. The nodes which could not establish a direct pairwise key enters into secure path discovery. If a node with common keys is captured by an attacker, it can effect other nodes which have not been captured with given probability. Few improvements to this scheme are given in [6], [7].

Asymmetric key management techniques require public key infrastructure (PKI) with certificate authority (CA) [8]. As the nodes are deployed at remote locations and due to paucity of resources, th nodes are unable to manage the certificates. Identity based encryption (IBE) scheme makes use of unique ID of the device as its public key [9]. The IDs are assigned to the nodes at the time of deployment ensuring their uniqueness. The IBK scheme does not need a CA, however it requires a private key generator (PKG), which is used to generate privRate keys based on the node ID. A WSN implementation of identity based cryptography based on IBE-trust security framework is given in [10]. In pairing based cryptography (PBC), a pair wise key between the nodes is made use of [11]. An ARM processor based implementation of pairing functions from MIRACL library is studied in [12], [13]. A pairing operation consumes maximum power about $0.444J$. Energy consumption and execution time of point operations over super singular elliptic curve is also presented. TinyPBC is a pairing algorithm for ID- based non interactive key distribution in WSNs [14]. It demonstrates how the nodes exchange keys in authenticated and non interactive manner. A symmetric key distribution scheme based on identity based cryptography (IBC) is presented in [15]. The asymmetric key algorithm, IBC is used for authenticated key agreement. Then encryption is performed using the symmetric keys generated. A balance between resilience and resource consumption between nodes can be achieved with the application of both symmetric and asymmetric key distribution techniques in hierarchical WSNs [16], [17], [18].

For heterogeneous WSNs, key management technique based on AVL tree [19] and Elliptic curve cryptography (ECC) is used to distribute keys with minimum resource requirements [20]. The cluster creation is secured by using master public/pair key calculated using elliptic curve. The cluster heads with durable batteries are decided before deploying the network. A framework for key pre-distribution scheme for heterogeneous WSNs is discussed in [21]. The scheme does not consider the hierarchical WSN. A group key distribution technique for hierarchical WSN is proposed in [22]. Different types of group keys are established for the nodes at various levels post deployment. ECC-based key management technique for hierarchical WSNs is proposed in [23]. The signcryption technique is used to secure channel between cluster head and the base station to provide forward secrecy. To circumvent the problem of node compromise, periodic authentication of the nodes is carried out.

III. Proposed key management

In hierarchical WSNs, the data is collected from the leaf nodes and aggregated by the CH nodes. The CHs send the data towards the BS. In multi-level hierarchical WSNs, the data can be aggregated further by CHs at the next level. The data value gets transcended as it moves to higher levels of hierarchy. In order to protect the data between CHs and the BS, an asymmetric key distribution technique is made use of in the proposed scheme. A probabilistic key pre-distribution scheme, which is less secure and consuming less resources, is used to establish shared keys between the CH and its leaf nodes. The ID- based shared keys, using bilinear pairing over elliptic curves, are established among the CHs and the BS. Pre-distributed key rings on each node are used to find shared keys between cluster head and sensor nodes inside the corresponding cluster. The motivation of the proposed technique is to provide balance between the resource consumption and security strength in hierarchical wireless sensor network. Figure 2 shows the structure of key management scheme.

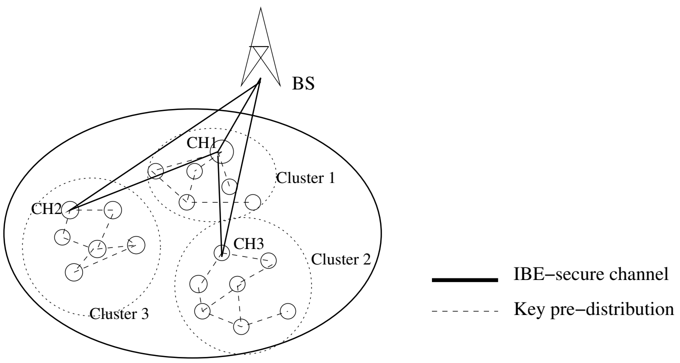

Fig. 2. Hybrid key management scheme

A. Set up phase

This work makes use of hierarchical WSN with homogeneous sensor nodes. During pre-deployment phase all the nodes are loaded with the same cryptographic primitives. The cluster heads are elected post-deployment. The BS is connected to a computer and it generates ID- based private keys for all the nodes in the network. ID-based private keys are calculated by scalar multiplication on elliptic curve [29],[30] of unique identity of the node and master key of the BS. A large pool of keys is generated by the BS and a randomly chosen set of keys is installed in each node. In order to support key distribution mechanism after deploying the network, the following parameters are loaded in each of the sensor nodes:

K_{ring_i} - Set of keys of node i for probabilistic key pre-distribution scheme
ID_i - Unique identity number of sensor node i.
K_{ID_i} - ID-based private key of node i
ID_{list} - List of identities loaded in each node
E_{param} - Elliptic curve parameters
e - Bilinear pairing function

978-1-4799-2027-3/14/$31.00 ©2014 IEEE

H_1 - Hash function to map node ID to elliptic curve point
H_2 - Hash function for cryptographic key calculation
$E_K()$ - Encryption function with key K

B. Secured clustering

The wireless network security is dependant upon the initial trust establishment among the nodes, the CHs and the BS. The implementation of secured clustering approach assures the initial security for WSNs.

C. Inter cluster key distribution

In the proposed protocol, a CH calculates the ID- based public key (U_{ID}) of the other CHs. The public key of CH j calculated by node i can be represented by using equation (1).

$$U_{ID_j} = H_1\left(ID_j\right) \tag{1}$$

After the calculation of public key, CH i computes the shared key by using pre-installed pairing algorithm, as given by equation (2).

$$K_{i,j} = e\left(K_{ID_i}, U_{ID_j}\right) \tag{2}$$

This shared key is same as the shared key computed by CH j using the unique identity CH i. This can be proved by using bi-linearity property of pairing algorithm as given by equation (3).

$$K_{j,i} = e\left(K_{ID_j}, U_{ID_i}\right) \tag{3a}$$

$$K_{j,i} = e\left(s.U_{ID_j}, U_{ID_i}\right) \tag{3b}$$

$$K_{j,i} = e\left(U_{ID_j}, s.U_{ID_i}\right) = K_{i,j} \tag{3c}$$

D. Intra cluster key establishment

A sensor node in a cluster communicates only to its CH. When a cluster is created during the initial stage, the CH broadcasts the identifiers of the keys from its key ring (Key_{ring}). Since only the key identifiers are transmitted, actual keys remain safe. If a sensor node finds the common key identifier, the corresponding key is used as the shared key for the communication between the leaf node and its CH. If no common key identifier between the leaf node and its CH exists, a path key is established between them with the help of another leaf node, which has been sharing a key already with the CH. In the proposed scheme, the path key discovery is limited to single hop, so as to avoid excessive communication. If a path key cannot be established in single hop, the CH establishes shared key with that node using ID-based key agreement technique to assure full connectivity. After shared key is established between the CH and the leaf node $k_{CH-Node}$.

$$K_{CH-Node} \leftarrow H_2(K_{CH_i} \oplus k_{CH-Node}) \tag{4}$$

E. Key update mechanism

In hierarchical WSNs, the energy in the CHs drains out soon due to additional work load of data aggregation and initial cluster set up. This work uses identical nodes. In order to avoid exhaustion of energy in a CH node, the CH role is rotated among the nodes in a cluster periodically. The sensor node having highest battery energy is selected as the new CH. At the time of selecting new CH, the keys inside the cluster are also updated. The older CH introduces the latest CH to the BS as well as to the other CHs. The latest CH carries out intra cluster key establishment mechanism again. The ID- based shared key of the cluster is updated consequently.

$$CH \rightarrow BS : E_{K_{CH,BS}}\,(\text{CLUSTER-INFO}) \tag{5}$$

IV. Implementation

The proposed key management scheme is implemented on IRIS hardware platform to check its feasibility in real world applications. IRIS mote with 8-bit ATMEGA1281 micro-controller and RF230 transceiver are used along with MDA100 sensor board. The only energy source of the nodes is two AA- size Alkaline batteries with 2000 mA-hr capacity. The RF230 transceiver works in 2.4 GHz frequency band and has variable transmission power level ranging from 3.2 dBm to -17 dBm. The MAC protocol used by these nodes is IEEE 802.15.4. Further, the nodes run TinyOS event based operating system specifically designed for WSN applications. The key management protocol is implemented in application layer using nesC programming language. The BS board MIB520 is connected to a computer.

The BS supports the private key generator and random key server. In the implementation of ID-based key management scheme, TinyPairing [31] cryptographic library has been made use of. TinyPairing library functions are loaded into each node before the deployment. Also, the BS uses the library functions to generate a master secret key (s) and a private key of each of the nodes. To run probabilistic key pre-distribution technique, the BS makes use of random number generator supported by the TinyOS. Initially, a key pool with $4,500$ keys is generated. A key ring is selected by the BS randomly and loaded in each of the nodes in the network. The Key ring size used in the implementation is 100 with each key of 160 bytes and identifier of size 2 bytes.

The key management application protocol is loaded in each of the nodes along with the *XMesh* multi-hop routing protocol. The *XMesh* is well tested dynamic routing protocol and implementation of security algorithm along with it inherently proves the feasibility of security algorithms in real world WSN applications. Table -I shows the total memory requirement when key management technique along with the *XMesh* protocol have been loaded into a node. The WSN implementation of an application involves all the operations of a node, which include sensing, routing and security algorithms.

TABLE I. Memory requirements for implementation on IRIS sensor node

Memory	Required	Available	% of Usage
ROM	115060 B	128 KB	87.78
RAM	5443 B	8 KB	66.44

A. Simulation model

A simulation model of the proposed scheme has been created using OmNET++ simulation platform [32] to study the overheads of the key management technique. The proposed key management protocol is written in the application layer using C++ modular approach. In the proposed scheme, key management technique is applied along with cluster formation and CH rotation. The network consists of a base station and wireless nodes. The wireless nodes deployed in the network are homogeneous, similar to the hardware implementation. IEEE 802.15.4 MAC layer protocol model has been used. The energy consumption model is based on current consumption specifications of IRIS node (used in the hardware implementation) [33].

V. Results and Analysis

A. Security analysis

Different key management related issues of the proposed technique are discussed as follows:

Scalability: The CH formation mechanism adopted in the scheme allows large number nodes to be deployed with reduced memory and energy overheads. The CH formation is secure and on line key calculation mechanism for new clusters can be easily added during the network lifetime.

Forward and backward secrecy: Since the CH role is rotated among the nodes, the secret keys related to each cluster are refreshed periodically. Hence, new nodes can not discover previous messages. The key reinforcement mechanism ensures that the keys related to the nodes in the lower hierarchical level are also modified.

Memory overhead: The memory overheads associated with the proposed scheme are higher than that of the probabilistic key distribution and identity based key management (IBK) techniques. Reduced computational and energy cost is compensated with additional memory overhead. Table -II provides a comparison of the memory overheads of IBK, probabilistic key pre-distribution and the proposed schemes.

TABLE II. Comparison of memory overheads for the key management schemes

Key scheme	Memory Overhead
Probabilistic	7 KB
IBK	28 KB
Proposed	38 KB

Energy consumption: A CH consumes most of its energy and there is a likelihood of a single node drains out its energy soon. In the proposed scheme, the energy consumption is distributed among all the nodes as the CH role is rotated among the nodes periodically, thereby conserving the energy. A simple key pre-distribution technique is applied for majority of the nodes, which requires less energy when compared with IBK. Also, energy is conserved by non-interactive key calculation at the CH level.

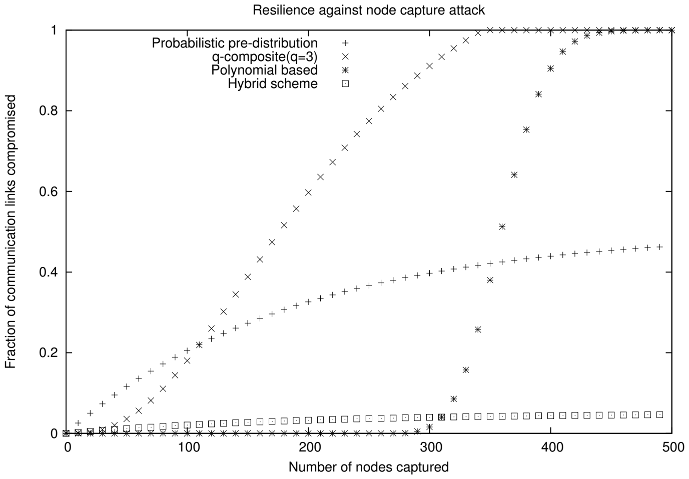

Fig. 3. Analysis of resilience against node capture attack [17]

TABLE III. Communication overheads and energy consumption of Proposed key management protocol

Phase of Operation	Bytes transmitted	Energy consumption
Initialization	24 Bytes	2.304 mJ
Shared key discovery	738 Bytes	70.848 mJ
Path key discovery	504 Bytes	48.384 mJ
Cluster head alteration	42 Bytes	4.032 mJ
Key update	1242 Bytes	119.232 mJ

B. Resilience against node capture

In WSN applications the nodes are openly deployed in the field and the chances of node capture are high. When a node is captured, in the case of probabilistic key pre-distribution scheme, the secret information about non-captured nodes is also revealed. In IBK technique, communication links between non-captured nodes are not compromised because of the discrete logarithmic problem imposed by bilinear pairing. In the proposed key management technique, communication links between non-captured nodes inside the cluster are effected. The key reinforcement ensures that the communication links outside the cluster are not compromised. The parameters used to carry out the analysis of the proposed key management scheme are:

Number of nodes in WSN: 1000
Number of nodes captured: 0 to 500
Number of clusters: 10
Connectivity probability: 0.5
Key pool size: 20000
Key ring size: 120

C. Communication overhead

Key management technique establishes initial trust in the network. Hence, messages exchanged in the network at the initial stage to distribute the keys are analysed. Energy consumption because of message exchange depends on the time spent in transmitting a message. The cluster formation and CH rotation processes require additional messages to be exchanged among the nodes. This communication overhead is compensated making used of the proposed key management protocol. Based on current specification of IRIS node and clock cycles required for wireless message transmission, the communication overheads are presented in Table -III.

D. Simulation results

The proposed key management technique is designed for hierarchical WSNs and hence overhead of cluster formation

TABLE IV. COMPARISON OF ASYMMETRIC KEY TECHNIQUES

Key scheme	Messages per shared key	Computational Time	Total Energy per shared key
ECDH	2	5.375 s	133.608 mJ
IBK	0	5.8066 s	130.5 mJ

along with the key management scheme is studied. The cluster formation and CH rile rotation model used for simulation is based on the residual energy of the node. The cluster formation is initiated by the BS and based on the distance metric, a CH selects its members in its cluster. In simulation model also, all deployed nodes are considered to be homogeneous with few nodes performing the duty of CHs. Periodically, CHs are rotated on the basis of the residual energy left with the nodes. The simulation parameters are as follows:

Number of nodes in the network: 12
Number of clusters: 3
Energy in each node: 10 J
Cluster head alteration period: 50 seconds
Sensor data collection interval: 5 seconds

Total energy in the node, the CH rotation rate and sensor data collection rate are selected for comparison of node lifetime. The hardware implementation parameters are different. Figure 4 shows the depletion in the energy of a nodes with time. The secure cluster formation and updates drain the energy sooner than that of a non-secure scheme.

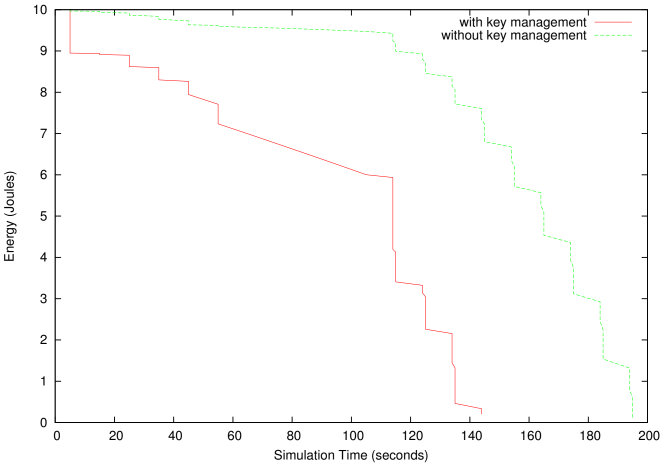

Fig. 4. Analysis of secure cluster head formation analysis

E. Comparison of asymmetric key techniques

At the CH level, the IBK is compared with ECDH key exchange mechanism [34] in Table IV. ID-based key management technique requires more time to compute shared key as pairing operation is involved but its non-interactive key agreement feature conserves energy. Further, ECDH is prone to 'Man in the middle' attack and hence IBK is proved to be more secure and energy conservative at the higher hierarchical level.

F. Overall energy overhead

The energy overheads due to communication and computational operations for the proposed key management scheme, IBK management scheme and probabilistic key pre-distribution scheme are compared in Table V. All the three key management protocols have been implemented using 12 IRIS sensor nodes and a cluster size of 4 is selected at the deployment time. The sensor nodes are deployed randomly and clusters are formed as given in the proposed scheme. The CH rotation and the key update mechanism processes are carried out after every 20 cycles of data aggregation.

TABLE V. ENERGY OVERHEAD KEY MANAGEMENT TECHNIQUES

Key scheme	Energy overhead
IBK	1149.70 mJ
Probabilistic key distribution	995.33 mJ
Proposed key management	277.16 mJ

VI. CONCLUSION

In WSNs, energy resource is a limiting factor, while designing communication and security protocols. In the proposed scheme, a combination of symmetric and asymmetric key primitives at different levels of hierarchy has been applied to minimise the energy overhead. The communication and computational operations consume most of the energy, when security protocols are applied to resource constrained sensor nodes. To minimize these overheads and at the same time to provide the required security level, the resource consuming IBK technique is applied between cluster heads and the base station only. The proposed key management technique proves to be better than the probabilistic key pre-distribution and the IBK techniques, when applied separately in the nodes. The secure cluster formation and key reinforcement mechanisms applied in this scheme restrict the node capture attack and other network attacks to the cluster alone.

REFERENCES

[1] K. Sohraby, D. Minoli, and T. Znati, *Wireless sensor networks: technology, protocols, and applications*. Wiley-interscience, 2007.

[2] A. Swami, Q. Zhao, Y.-W. Hong, and L. Tong, *Wireless Sensor Networks: Signal Processing and Communications*. Wiley, 2007.

[3] E. Upton and G. Halfacree, *Meet the Raspberry Pi*. Wiley, 2012.

[4] J. Lee, V. Leung, K. Wong, J. Cao, and H. C. B. Chan, "Key management issues in wireless sensor networks: current proposals and future developments," *Wireless Communications, IEEE*, vol. 14, no. 5, pp. 76–84, 2007.

[5] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM conference on Computer and communications security*. ACM, 2002, pp. 41–47.

[6] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*. IEEE, 2003, pp. 197–213.

[7] A. Rasheed and R. Mahapatra, "Key predistribution schemes for establishing pairwise keys with a mobile sink in sensor networks," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22, no. 1, pp. 176–184, 2011.

[8] S. William *et al.*, *Cryptography and Network Security, 4/e*. Pearson Education India, 2006.

[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[10] Y. Yussoff and H. Hashim, "Ibe-trust: A security framework for wireless sensor networks," in *Internet Security (WorldCIS), 2011 World Congress on*, 2011, pp. 171–176.

[11] S. D. Galbraith, K. G. Paterson, and N. P. Smart, "Pairings for cryptographers," *IACR ePrint Archive*, 2006.

[12] B. Doyle, S. Bell, A. Smeaton, K. Mccusker, and N. O'Connor, "Security considerations and key negotiation techniques for power constrained sensor networks," *The Computer Journal*, vol. 49, no. 4, pp. 443–453, 2006.

[13] M. Scott, "Miracl–multiprecision integer and rational arithmetic c/c++ library," *Shamus Software Ltd, Dublin, Ireland, URL¡ http://www. shamus. ie*, 2003.

[14] L. Oliveira, M. Scott, J. Lopez, and R. Dahab, "Tinypbc: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," in *Networked Sensing Systems, 2008. INSS 2008. 5th International Conference on*, june 2008, pp. 173 –180.

[15] K. McCusker and N. O'Connor, "Low-energy symmetric key distribution in wireless sensor networks," *Dependable and Secure Computing, IEEE Transactions on*, vol. 8, no. 3, pp. 363 –376, may-june 2011.

[16] M. Rahman and S. Sampalli, "A hybrid key management protocol for wireless sensor networks," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012, pp. 769–776.

[17] R. K. Kodali and S. Chougule, "Hybrid key management technique for wsns," in *Quality, Reliability, Security and Robustness in Heterogeneous Networks*. Springer, 2013, pp. 854–865.

[18] R. Kodali, S. Chougule, and A. Agarwal, "Key management technique for heterogeneous wireless sensor networks," in *TENCON Spring Conference, 2013 IEEE*, 2013, pp. 183–187.

[19] Y.-Y. Zhang, W.-C. Yang, K.-B. Kim, and M.-S. Park, "An avl tree-based dynamic key management in hierarchical wireless sensor network," in *Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP'08 International Conference on*. IEEE, 2008, pp. 298–303.

[20] H. Boumerzoug, B. Amar Bensaber, and I. Biskri, "A key management method based on an avl tree and ecc cryptography for wireless sensor networks," in *Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks*. ACM, 2011, pp. 57–62.

[21] K. Lu, Y. Qian, M. Guizani, and H.-H. Chen, "A framework for a distributed key management scheme in heterogeneous wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 2, pp. 639–647, 2008.

[22] B. Panja, S. Madria, and B. Bhargava, "Energy and communication efficient group key management protocol for hierarchical sensor networks," in *Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006. IEEE International Conference on*, vol. 1, 2006, pp. 8 pp.–.

[23] M. Alagheband and M. Aref, "Dynamic and secure key management model for hierarchical heterogeneous sensor networks," *Information Security, IET*, vol. 6, no. 4, pp. 271–280, 2012.

[24] V. S. Miller, "The weil pairing, and its efficient calculation," *Journal of Cryptology*, vol. 17, no. 4, pp. 235–261, 2004.

[25] M. Scott, "Computing the tate pairing," in *Topics in Cryptology–CT-RSA 2005*. Springer, 2005, pp. 293–304.

[26] P. Barreto, S. Galbraith, C. hÉigeartaigh, and M. Scott, "Efficient pairing computation on supersingular abelian varieties," *Designs, Codes and Cryptography*, vol. 42, no. 3, pp. 239–271, 2007.

[27] D. Freeman, "Constructing pairing-friendly elliptic curves with embedding degree 10," in *Algorithmic number theory*. Springer, 2006, pp. 452–465.

[28] F. Brezing and A. Weng, "Elliptic curves suitable for pairing based cryptography," *Designs, Codes and Cryptography*, vol. 37, no. 1, pp. 133–141, 2005.

[29] R. K. Kodali, K. H. Patel, and N. Sarma, "Energy efficient elliptic curve point multiplication for wsn applications," in *Communications (NCC), 2013 National Conference on*. IEEE, 2013, pp. 1–5.

[30] R. K. Kodali and H. S. Budwal, "High performance scalar multiplication for ecc," in *Computer Communication and Informatics (ICCCI), 2013 International Conference on*. IEEE, 2013, pp. 1–4.

[31] X. Xiong, D. S. Wong, and X. Deng, "Tinypairing: a fast and lightweight pairing-based cryptographic library for wireless sensor networks," in *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*. IEEE, 2010, pp. 1–6.

[32] A. Varga *et al.*, "The omnet++ discrete event simulation system," in *Proceedings of the European Simulation Multiconference (ESM2001)*, vol. 9. sn, 2001.

[33] A. Sivagami, K. Pavai, D. Sridharan, and S. S. Murty, "Estimating the energy consumption of wireless sensor node: Iris," *International J. of Recent Trends in Engineering and Technology*, vol. 3, no. 4, 2010.

[34] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*. IEEE, 2005, pp. 324–328.