Threshold Cryptography Based Light Weight Key Management Technique for Hierarchical WSNs

K. Hamsha(✉) and G. S. Nagaraja

R V College of Engineering, Bangalore 560059, Karnataka, India
hamshak@gmail.com, nagarajags@rvce.edu.in

Abstract. Secure communication among sensors is strongly needed to avoid malicious activity. Security is a major issue in self-organized, infrastructure less networks with limited resources such as energy, transmission range, and processing. The amount of network overhead needs to be reduced to improve the network performance. The size of the secret key to be communicated among the sensor nodes is also contributing in network performance. The Proposed Light Weight Threshold Key Management Scheme (LWKMS), reduces the size of the secret key to be communicated. It reduces the network resource utilization, in sharing the secret among the sensor nodes in the network and provides efficient security even when the keys are compromised by an attacker node. Simulation results shows that the proposed light weight scheme provides less overhead along with less energy consumption as compared to existing method namely Group Key Management Scheme (GKMS).

Keywords: Light weight key management · Secure hierarchical networks · Threshold cryptography · WSN

1 Introduction

Wireless Sensor Networks (WSN) [1] are used for a wide variety of applications ranging from target detection to environment modeling. The network performance gain and QOS are important entities for WSNs. WSN are exposed to various attacks and also there is much malicious intent which occurs. Establishing a secure channel of communication is a demanding task [2]. The major challenge is to secure data transmission with more integrity and confidentiality constraints [3]. Data collection cycle performs round transmissions between the Base Station (BS) and other sensor nodes (SN) in the network. In order to reduce the number of control packets for a given data packet gathering is used by BS [4–6]. There are many encryption and decryption schemes which have been suggested by various researchers. Key management layer is responsible for the generation of keys, distribution of keys, revocation of keys among sensing device [7].

Cryptographic methods for WSNs has been proposed by authors [8, 9] which adopts hierarchical architecture for secure communication. In secret sharing scheme proposed by authors [10, 11] employs secret key distribution into nodes, to generate

N. Kumar and R. Venkatesha Prasad (Eds.): UBICNET 2019, LNICST 276, pp. 188–197, 2019.
https://doi.org/10.1007/978-3-030-20615-4_14

and assign keys. However these schemes consume more energy, large memory space and high communication overhead in exchanging messages to establish key system.

LWKMS is used in this work. The BS is responsible for distributing the Secret Key Shares (SKS) among a set of n chunks for CH, CH will perform data gathering from normal nodes and then establishes a route to BS. The scheme with threshold enables secure data transmission to BS. During the routing process, CH will communicate with other CHs to send the packets to BS.BS generates and computes key value and sends it to CH,CH will divide that into different payloads and then shares among the participants by estimating the threshold value.

This work is organized in the following fashion; Sect. 2 describes the related work and problem statement. Sections 3 and 4 describes the proposed system model. In Sect. 5 the performance analysis and relative simulation are conducted. Finally, we draw the conclusion on the proposed scheme in Sect. 6.

2 Related Works and Problem Statement

Many researchers attempted to present security mechanism for WSNs [12–16]. Cryptography based security protocol using public key and other key management methods. These security protocols are attempts to provide security in flat routing for WSNs. The security in hierarchical routing is less addressed than the flat routing for WSNs. Problem in group key management scheme; mutual authentication is performed by using asymmetric key protocol between high and middle powered nodes and establishes links to groups. Once a forwarding node is tampered then security information of entire zone will be leaked. Traditional Shamir's secret key sharing mechanism for hierarchal group based scheme consumes huge storage and computational cost which incurs more networks overhead.

Lu et al. [17] makes use of ID-based digitally signed key for establishing a secure routing for a zone based network. In ID based method, for all the nodes received signal strength (RSS) is computed and then a node with highest value is chosen as region head.. Cluster head communicate directly to base station. The node id will generate public key and private keys without making use of supplementary data transmission techniques in the proposed method. Even though the proposed technique has security efficiency, it exhibits high computational cost. Bertier [18] presented secret key sharing scheme by providing basic secret keys sharing without cryptography between nodes to establish secure communication among neighbor nodes. The author extended work on establishing secret key exchange algorithm, however this scheme consume more energy for key exchange and authentication process which made it unsuitable. Claveirole [11] proposed aggregation based method to secure data on secret sharing to mitigate from DoS attack by splitting message and forwarding these messages through multiple path. This scheme confuses the adversary in finding the actual route. Qin [19] proposed light weighted authentication key management scheme (AKMS), where keys are dynamically generated. Attackers cannot reuse the previous key to cheat. This scheme offers high security with low cost to solve malicious activity in network. This scheme contains three phases, key pre distribution phase where symmetric network key is generated and stored. Network initialization phase, where nodes find its neighbors within communication range and authentication phase involves authenticating and verifying nodes. Chen [20] proposed trust aware low energy security protocol, which considers node's trust values in building topology. This combines trust value, node density and residual energy to select cluster head.

3 Network Model

Network consists of WSNs nodes which are hierarchically clustered. The cluster head is responsible to collect data from cluster members and aggregate the data and forward the aggregated data to BS. Network consists of WSNs nodes which are hierarchically clustered.CH will obtain the payloads from normal nodes (NN) and then relays it to BS. The transmission efficiency is obtained by using more bandwidth and transmission power for CH. The network distribution model is represented in Fig. 1. The BS initially is responsible for distribution of shared secret key k from the sequence $k_0, k_1, k_2.\ldots..k_{n-1} \in \{0, 1\}$ where k represents regular or partitioned secret key. BS is equipped with sufficient energy and resources, it keeps all ID's and Keys. Using Shamir's threshold secret key scheme (t, n) on Lagrange polynomial interpolation.

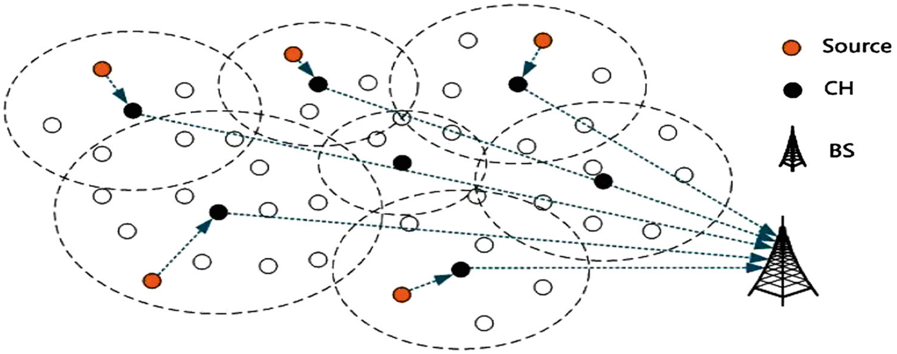

Fig. 1. Network architecture

In threshold secret key scheme BS assigns secret keys and data to each sensor nodes, but does not reveals the secret data. Initially there are p players and a trusted authority $T_a, U = \{p_1, p_2.\ldots..p_n\}$. The method makes use of two phases namely Key generation and construction phase.

3.1 Key Generation Phase

A random polynomial of degree of $f(x)$ *of* $(t-1)$ is selected by the trusted authority T_a

$$f(x) = S + a_1x + \ldots + a_{t-1}x^{t-1}(modP), \quad (1)$$

Consider a finite set of co-efficient with p players represented as $S, a_1, a_2, \ldots., a_{t-1}$ for a condition $secret = f(0)$.

The shares $S_i = f(x_i)$ are computed by the trusted authority and further S_i are privately distributed to each player, which falls under the trusted authority T_a.

3.2 Construction Phase

Shares of $S_1, S_2, \ldots..S_t$ of, secret key S can be constructed as

$$f(x) = \sum\nolimits_{i=1}^{t} S_i \left(\prod\nolimits_{i \neq j} \frac{x - x_j}{x_i - x_j} \right) (modP) \tag{2}$$

$$f(x) = \sum\nolimits_{i=1}^{t} S_i \left(\prod\nolimits_{i \neq j} \frac{x_j}{x_j - x_i} \right) (modP) \tag{3}$$

The following assumptions are used in modeling of the network

Sensor nodes are static.
Base station assigns unique ID for each sensor.
All sensor nodes are homogenous.
Compromise node reveals all the keys.

4 Proposed Hierarchal Threshold Scheme

We use Shamir's scheme to distribute shares of an initial secret α with threshold among players $P = (p_1, p_2, p_3, \ldots\ldots p_n)$. Suppose the levels are $L = (l_1, l_2, l_3 \ldots..l_n)$ with set of players $\{n_1, n_2, n_3, \ldots.n_n\}$ and threshold $\{t_1, t_2, \ldots..t_n\}$ corresponding to field F.

4.1 Sharing Phase

The BS uses polynomial method for sharing of random secret key with threshold dynamically at each level.

(1) The BS, makes use of polynomial method to generate the shares of random secret β_i with threshold $t \in \min\,[t_i, t_{i+1}, t_{i+2} \ldots t_m]$.
(2) Cluster members n_i will keep the shares of β_i as their final shares $p = p - \{n_i\}$
(3) The Lagrange method is used to change the threshold dynamically at each level for each level of the sensor node $i \in [i, m-1], \propto_{i+1} = \propto_i + \beta_i$ and calculation of $\{\propto_1, \propto_2, \propto_3, \ldots, \propto_m\}$ happens before α_m.

4.2 Recovering Phase

At recovery phase all secret keys are collected at each level for the master secret key. All secret keys are recovered at base station by solving linear congruence.

(1) Collect the each hierarchy level secrets, $\propto_m$ from level m, β_{m-1} to level $(m-1), \beta_{m-2}$ from level $(m-2)\ldots.\beta_1$ to level 1 for the recovery of the master secret.

(2) At every level of hierarchy of WSNs, the recovery of secret is done using

(3) Lagrange interpolation method with $Secret_i = \sum_{j\in\Delta_i} (\gamma_j^{\Delta_i} X \varphi_j)$

(4) All the secret keys are recovered at the base station by solving the linear congruence's $\alpha_{i+1} = \alpha_i + \beta_i$ mod q for $i = (m-1)$ down from level $i = 1$. Hence $\propto_{m-1}, \propto_{m-2}, \ldots, \propto_1$ are used.

4.3 Network Initialization Phase

The network key (n_k) is preloaded for all the nodes in the network. The n_k is a symmetric encryption key generated using Elliptical Curve Cryptography (ECC). By using n_k all the messages are transmitted by the senor nodes. The cluster formation of nodes in hierarchical network and the selection of CH among the nodes in the cluster are done by using LEACH protocol.

By sending its id and current time stamp c_t the CH performs pairwise key generation request k_{req} to BS. Upon receiving the pairwise key generation request BS generates $'p'_k$ pairwise key using one way hashing $'H'$ as

$$P_k = H(CH_i \oplus BS \oplus C_t) \tag{4}$$

BS encrypts the p_k sends to CH_i

$$BS \rightarrow CH_i = k_{reply}(CH_i, BS, E(C_t \| p_k)) \tag{5}$$

4.4 Intra Cluster Pairwise Key Generation

The intra cluster pairwise key is used to communicate between sensor nodes and CH.

The cluster head CH_i soon after elected as cluster head, then the cluster head CH_i checks its Cluster Member (CM) list $CM_{list} = \{CH_{iN_1}, CH_{iN_2}\ldots\ldots\ldots CH_{iN_m}\}$ where m represents the total no of nodes present in the list. BS receives the node list from the CH_i of each cluster.

$$CH_i \rightarrow BS : \{CH_i, BS, CM_{list}, C_t\} \tag{6}$$

The combination of pairwise key and one way hash function is used by the base station to compute the cluster key CH_k in such way that $CH_iBS \rightarrow CH_i : [CH_i || \mathrm{I}_{p_k}, (N || \{CH_{iN_1}, CH_{iN_2}, \ldots, CH_{iN_m}\})]$ And then cluster head CH_i finally sends to its cluster members nodes

$$CH_i \rightarrow N_i : \{CH_i || CH_{iN_1} || C_t\} \tag{7}$$

CH_i will share the secret keys S_i to each node N_i in the cluster.

5 Simulation Results

The proposed scheme is evaluated and discussed in this section; our scheme is to solve the security issues and to provide light weighted key management system to reduce the network overhead. Proposed light weighted threshold key scheme (LWKMS) is compared with the Hierarchal group key management scheme (GKMS). The proposed method is evaluated for network parameters like packet delivery ratio, energy consumption and network overhead. The network security issues are analyzed by introducing attacker nodes into the network. The attacker nodes are varied in different rounds. The above said proposed scheme is simulated using event driven simulator NS2 with the network simulation parameters described in Table 1.

Table 1. Network simulation parameters

Network simulation parameters	Values
Deployment area	1000 * 1000 m
No of nodes	80
Bandwidth	2 Mb
Traffic type	CBR
Transmission range	250 m
Attacker nodes	2 to 10
Initial energy	30 J
Propagation model	Two ray model
MAC type	802.11
Protocol	LEACH

The deployment area which is taken into consideration is of dimensions 1000 * 1000 with 80 nodes which are randomly spread in the given area. For each sensor, the transmission range used in 250 m and number of attacker nodes taken into consideration are from 2 to 10. Each of the nodes is equipped with an initial energy of 30 J with propagation model taken into consideration is Two Ray Model with LEACH protocol.

In WSN, the attacks are possible due to open environment and node leaving or joining the network. Attacking the network requires node to be participate in network by doing malicious activities, which intrude the network. Node can also update false information of having shortest route to destinations and generate fake multiple identities. In our proposed scheme, we authenticate false node identities by a Sybil node, where it creates multiple identities and duplicates itself as authentic node. The proposed scheme can efficiently detect malicious node by its authentication and encryption technique.

Figure 2 below shows the detection of malicious activity by dropping the packets. The drop ratio increases in the group key management compared to threshold key scheme. The simulation result of packet delivery ratio is plotted in presence of attacker node, the attacker nodes try to misbehave and drop the packet. Using threshold cryptography the BS reconstructs data sent from sensor nodes, the identification of legitimate node which has shared secret key cannot be replay by malicious nodes to BS. LWKMS reduces error packets and forwards legitimate packet compared to GKMS where the complete group becomes compromise if attacked.

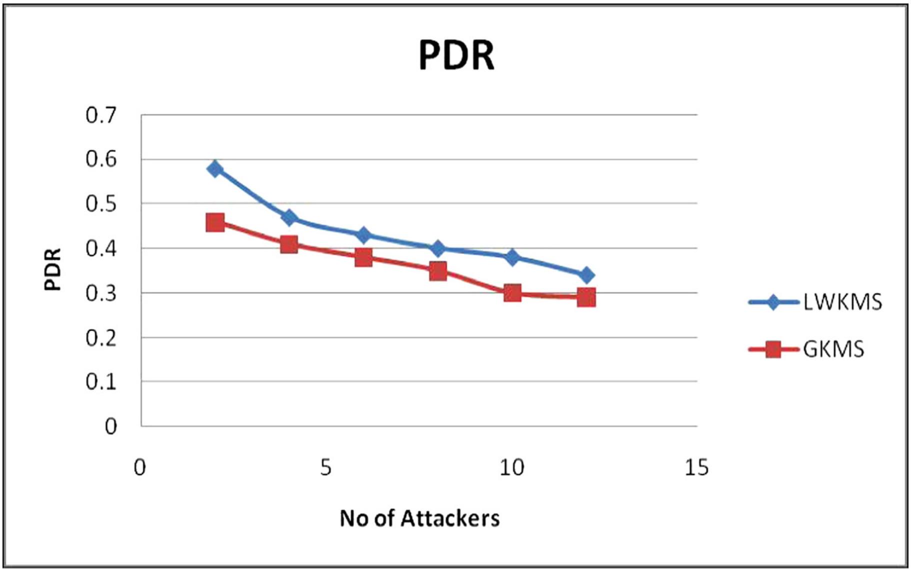

Fig. 2. Packet delivery ratio

In order to prolong the network lifetime node energy consumption has to be optimized, CM has the information about energy levels of other nodes and hence can select CH based on residual energy levels. CH energy depletes as the CH involves in authenticating itself to BS and controlling the CM. Figure 3 shows the average energy consumption of group key management scheme (GKMS) and proposed light weighted key scheme (LWKMS) for LEACH protocol.

The amount of energy consumed during the transmission and reception of data is used to calculate the average energy. The graph of network overhead below shows the average energy consumption of GKMS and LWKMS. Due to more error packets in the cluster energy drain rate increases, when the number of attacker nodes increases. CH filters error packets based on LWKMS and secures the group members and avoids spreading of error packets throughout the network. In GKMS when the attacker node is detected, the CH initiates new key generation procedure to BS which consumes more energy and assigns new keys to group. Proposed LWKMS consume less energy in presence of malicious node, by detecting malicious activity efficiently and does not allow participation of malicious activity in network. The average energy consumption, of the proposed system increases network lifetime. Since the light weighted threshold key management scheme requires time specific mode in authenticating nodes and hence LWKMS Consumes less resource and authenticates efficiently.

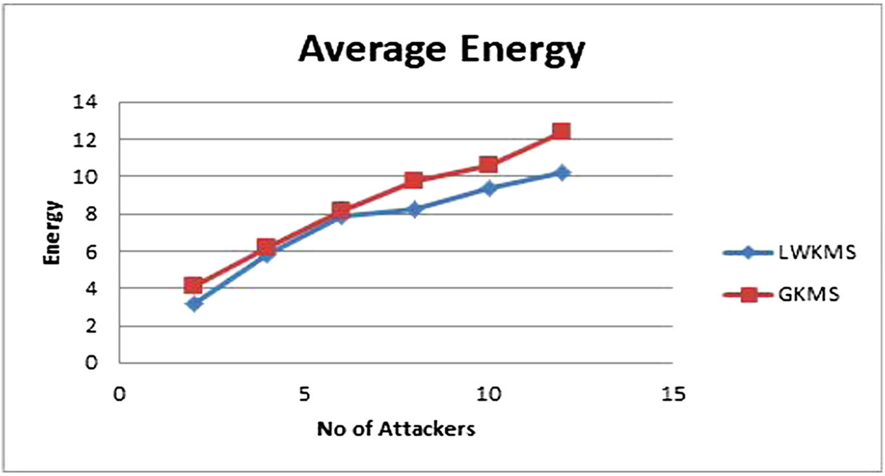

Fig. 3. Average energy consumption

Finally the overhead of the network is evaluated and shown in the network overhead graph as mentioned in Fig. 4. The key length of 256 bit key has been used to generate the graphs of key generation and key management schemes as shown in Fig. 5. LWKMS reduces the network overhead by generating shared keys and authenticating nodes by dynamically changing threshold using Lagrange interpolation, thus uses less resource and increases the network lifetime of the nodes.

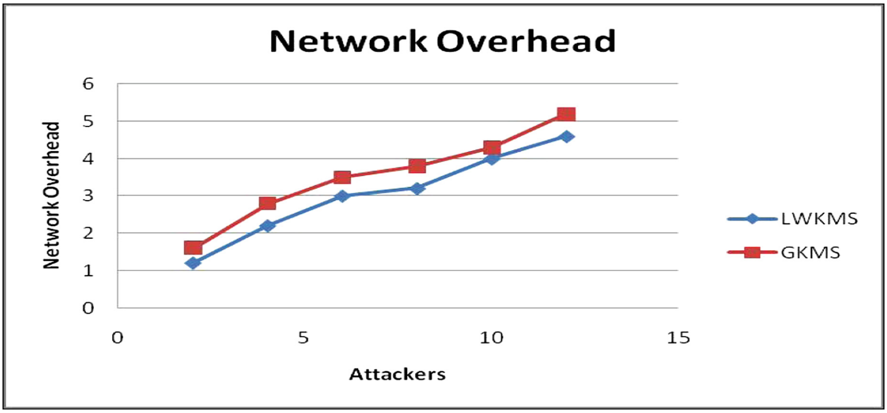

Fig. 4. Network overhead

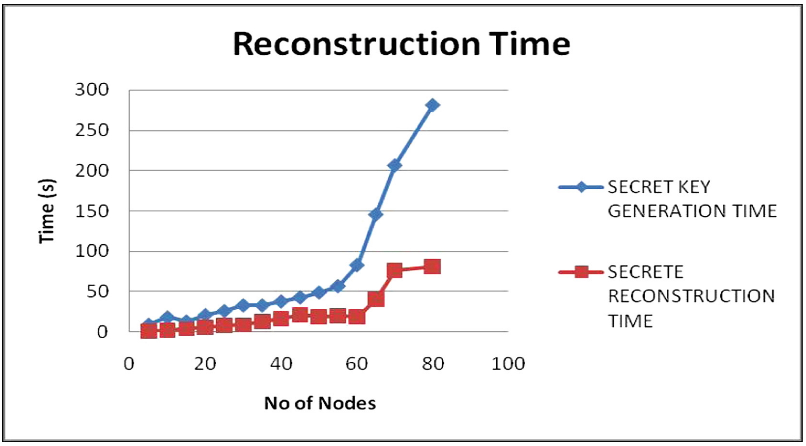

Fig. 5. Key reconstruction time

6 Conclusion

To enhance network security of resource constrained WSN, we propose light weight threshold key management technique using threshold cryptography. The Hierarchical network architecture is employed to provide secure data transmission to BS and node authenticity. We address security issues which increase network overhead in key sharing mechanism. We present LWKMS (Light weighted threshold Key Management Scheme) based on secret key sharing to authenticate nodes at each level by changing the threshold dynamically by Lagrange method at each level of the sensor node. Finally, the BS recovers all the shared keys to provide message confidentiality and authenticity. Less network overhead, high packet delivery ratio and lower energy consumption are obtained by proposed LWKMS method when compared with GKMS as shown in the simulation results. In future, robust routing in ubiquitous network to resist various attacks can be focused.

References

1. Akyildiz, F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Comput. Netw. **38**(4), 393–422 (2002)
2. Papalexakis, E.E., Beutel, A., Steenkiste, P.: Network anomaly detection using co-clustering. In: Proceedings of International Conference on Advances in Social Networks Analysis and Mining (ASONAM), pp. 403–410 (2012)
3. Zhou, L., Haas, Z.J.: Securing ad hoc networks. IEEE Netw. Mag. Glob. Internetworking **13** (6), 24–30 (1999)
4. Cai, Z., Ji, S., He, J.S., Bourgeois, A.G.: Optimal distributed data collection for asynchronous cognitive radio networks. In: Proceedings IEEE 32nd International Conference of Distributed Computing Systems, pp. 245–254 (2012)

5. Ji, S., Cai, Z.: Distributed data collection and its capacity in asynchronous wireless sensor networks. IEEE Trans. Parallel Distrib. Syst. **25**(8), 2113–2121 (2014)
6. Ji, S., Beyah, S., Cai, Z.: Snapshot/continuous data collection capacity for large-scale probabilistic wireless sensor networks. In: Proceedings IEEE INFOCOM, pp. 1035–1043 (2012)
7. Lee, J.C., Leung, V.C.M., Wong, K.H., Cao, J., Chan, H.C.B.: Key management issues in wireless sensor networks: current proposals and future developments. IEEE Wirel. Commun. **14**(5), 76–84 (2007)
8. Zhang, Y.Y., Li, X.Z., Liu, J.M., Yang, J.C., Cui, B.J.: A secure hierarchical key management scheme in wireless sensor network. Int. J. Distrib. Sens. Netw. (2012). Article ID 547471
9. Seyed, H.N., Amir, H.J., Vanesa, D.: A distributed group rekeying scheme for wireless sensor networks. In: Proceedings of the 6th International Conference on Systems and Networks Communications (ICSNC 2011), pp. 127–135 (2011)
10. Bertier, M., Mostefaoui, A., Tredan, G.: Low-cost secret-sharing in sensor networks. In: Proceedings of the IEEE 12th International Symposium on High Assurance Systems Engineering (HASE 2010), pp. 1–9 (2010)
11. Claveirole, T., Dias De Amorim, M., Abdalla, M., Viniotis, Y.: Securing wireless sensor networks against aggregator compromises. IEEE Commun. Mag. **46**(4), 134–141 (2008)
12. Nair, P., Cam, H., Ozdemir, S., Muthuavinashiappan, D.: ESPDA: energy - efficient and secure pattern based data aggregation for wireless sensor networks. In: Computer Communications IEEE Sensors, vol. 2, pp. 732–736 (2006)
13. Ahmad, M., Habib, M., Muhammad, J.: Analysis of security protocols for wireless sensor networks. In: Proceedings of 3rd International Conference on Computer Research and Development (ICCRD), vol. 2, pp. 383–387 (2011)
14. Castelluccia, C., Chan, A.C.-F., Mykletun, E., Tsudik, G.: Efficient and provably secure aggregation of encrypted data in wireless sensor networks. ACM Trans. Sens. Netw. (TOSN) **5**(3), 20 (2009)
15. Pathan, A.K., Hong, C.S.: SERP: secure energy-efficient routing protocol for densely deployed wireless sensor network. Annales des Telecomm **63**(9–10), 529–541 (2008)
16. Lin, K., Lai, ChF, Liu, X., Guan, X.: Energy efficiency routing with node compromised resistance in wireless sensor networks. Mob. Netw. Appl. **17**(1), 75–89 (2012)
17. Lu, H., Li, J., Kameda, H.: A secure routing protocol for cluster-based wireless sensor networks using ID-based digital signature. In: IEEE Global Communication Conference (2010)
18. Bertier, M., Mostefaoui, A., Tredan, G.: Low-cost secret sharing in sensor networks. In: Proceedings of the IEEE 12th International Symposium on High Assurance Systems Engineering (HASE 2010), pp. 1–9 (2010)
19. Qin, D., Jia, S., Yang, S.: A lightweight authentication and key management scheme for wireless sensor networks. J. Sens. **2016**, 9 (2016). Article ID 1547963
20. Chen, Z., He, M.: Trust-aware and low energy consumption security topology protocol of wireless sensor network. J. Sens. **2015**, 10 (2015). Article ID 716468