International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 8, August 2017

ISSN: 2394-4404

Cluster Based Secure Dynamic Keying Technique For Heterogeneous Mobile Wireless Sensor Networks

Ms. Gauri P. Heda

Prof. P. P. Rokade

Dept. of Computer Engineering, S.N.D.C.O.R.C, Yeola,
Dist-Nashik, Maharashtra, India

Abstract: ***Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. High level of security is provided. . The capabilities of the nodes depend on the type of network the node is residing in. Whatsoever may be the network efficiency, security is most important, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications. A secure mobility aware dynamic keying technique for authentication in WSN is proposed in this paper.Weightvalue is estimated using parameters such as the node degree, average distance, node's average speed, and virtual battery power. The keys are dynamically generated and used for providing security.The results show that the proposed methodologies have better performance.***

Index Terms: Cluster-based WSNs, Weight, heterogeneous, Secure data transmission, Dynamic key.

I. INTRODUCTION

A Wireless sensor network is built by various distributed devices which comprises of wireless sensor nodes by which physical or environmental are monitored. The single nodes in wireless sensor network can sense the environment. Nodes are also able of processing the information data and also sending data to one or more collection in a wireless sensor network [1]. There are different types of wireless sensor network. The capabilities of the nodes depend on the type of network the node is residing in. Whatsoever may be the network efficiency, security is most important, many WSNs are deployed in harsh, neglected, and often adversarial physical environments for certain applications, such as military domains and sensing tasks with trustless surroundings [2]. Mobility is also one the aspects of wireless sensor network (WSN) especially heterogeneous wireless sensor network (H-WSN)[3][4]. Mobility of the nodes has become essential in various applications. Researchers have investigated cluster based data transmission which increases the scalability of the network. Due to mobility clustering should be made dynamically. In a cluster-based WSN (CWSN), every cluster has a head sensor node, which is cluster head (CH). A CH aggregates the data collected by the leaf nodes (non-CH sensor nodes) in its cluster, and sends the aggregation to the base station (BS). The low-energy adaptive clustering hierarchy (LEACH) protocol presented by Heinzelman et al. [14] is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. Mobility of may cause malicious nodes and it may happen that malicious node may become head or cluster member. That gives malicious node the right of controlling the network. Hybrid, Energy-Efficient, Distributed Clustering (HEED) [5], Energy efficient heterogeneous clustered scheme (EEHC) [6], Stochastic Distributed Energy- Efficient Clustering (SDEEC) [7], Unequal clustering algorithm [8] are faced attacks on clustering. Enabling security in WSNs in challenging because the density, size of the network and also resource constraint in nodes. As WSNs are deployed in harsh, neglected, and often adversarial physical environments as providing physical security becomes impossible and difficult to predict. Data confidentiality, integrity, authenticity and availability are

considered to be the security requirements which the WSN should provide even in the presence of powerful attackers [12]. There are various threats and challenges which is to be solved.

The rest of this paper is organized as follows. In Section 2, the related works are discussed. Section 3 describes the cluster based secure dynamic keying technique which includes dynamic clustering, dynamic key management, authentication technique and bidirectional malicious node detection technique. Section 4 presents the results of the proposed work, section 5 concludes the paper.

II. RELATED WORK

H-WSN are disruption of cooperative transmissions which include routing attacks, jamming of signals, Wormhole attack, selfish behavior, resource draining attack, relay discovery attack, traffic injection attack, query flooding attacks, Sybil attack, bad mouthing attack, rushing attack [13]. Nodes in the network share a session key which is secret encryption key. Re-keying is performed using the other administrative keys and the new keys should not be known to the compromised node[17] When there is node compromise, node addition, node failure or when topology changes. Reasons for the node failure may be the malicious behavior or battery exhaustion. When forcefully a node leaves the network all the known keys to that node have to be changed[15][16]. In [12] pairwise keying model is more robust against the node capture attack as the other nodes are affected due to compromise of the single node. In [14] a protocol was presented which is a widely known and effective one to reduce and balance the total energy consumption for CWSNs. For prevention of energy consumption of set of CHs LEACH rotates randomly. Network lifetime was increased by LEACH. Later other protocols came as APTEEN[18] and PEACH[19]. LEACH-like protocols is challenging because they dynamically, randomly, and periodically rearrange the network's clusters and data links [21]. There are more secure protocol as Sec LEACH [21], GS-LEACH [22], and RLEACH [23].In S. Sharma et al.[24]orphan node problem arises where symmetric key management is applied. Orphan node problem occurs when a node does not share pair wise key with others in its pre loaded key ring. To mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pairwise symmetric keys with all of the nodes in a network. It cannot participate in any cluster, and hence elected as CH. Orphan node problem reduces the possibility reduces the possibility of a node joining, it also increases the overhead of transmission and energy consumption. The feasibility of the asymmetric key management shown in WSNs which compensates the shortage from applying the symmetric key management for security [25]. In [26]cryptography in asymmetric key management system offers digital signature where the binding between public key and the identification of the signer is obtained by digital certificate[26]. The identity-based digital signature (IBS) scheme is proposed by the author in[27].In[28] author has combined the benefits of IBS and key predistribution set into WSNs, later more work was done the same. In[29] author has came up with a general method for constructing signature schemes and IBOOS scheme was proposed to reduce the computation and storage costs of signature processing. In WSN, IBOOS scheme can be effective for key management.

III. CLUSTER BASED SECURE DYNAMIC KEYING TECHNIQUE

A method has been proposed to overcome the problem definition. A proposed method for authentication is secure dynamic keying based on cluster. This method deals with malicious node detection technique and mobility. In CSDKT,

In the CSDKT, after deployment of node in the field, CHs are selected based on dynamically calculated weight values. The GPS enabled heterogeneous nodes having high power. The weight values is estimated and the node having minimum weight value are chosen. The dynamic parameters such as node degree, virtual battery power, neighbor's average distance and average speed. Each node in the network calculates combined cost value and further this calculated value is used for the derivation of dynamic key. This dynamic key is used in communication for protecting the data and updated regularly based on the change in combined cost value. For the security within the network mobility of cluster members and CHs are performed by authentication using the dynamic key. The cluster members takes the responsibility of the CH re-election when it tends to leave the network. For the elimination of CH and malicious cluster member present within network a bidirectional malicious node detection technique is implemented. The number of CH depends on the size if the network. The processing ability, energy and memory of CH are high as compared to SN. SN collects the information and forward it to the CH. CH uses threshold secret sharing algorithm for splitting the packet into number of shares and forwards them to the sink via multiple link when it wishes to send the data to the sink[16]. The routing techniques are Multi-path dispersal routing [32]. The user communicates from BS as it is static while CH and SNs can move. BS is where CH sends the data and analysis is performed if required.

A. DYNAMIC CLUSTERING

a. VIRTUAL BATTERY ESTIMATION

Packet drop is resultant of synchronization issue so virtual battery power is considered. In initially deployment of SN, VBP value is assigned. CH nodes are assigned with more VBP as they have high configuration. During intra-cluster communication nodes transformation states are node-stay-alive, packet transmission as well as reception, encoding and decoding. While transmitting through states SN sends data into the network. When a source node detects any event, it forwards the packet size (Z) towards the sink. VBP can be updated cording to the cost associated with the actions performed then the V_{ci} is calculated. After every action the value of the VBP changes as the cost associated to that node also changes so, its transient value is obtained.

b. ELECTION OF CH AND FORMATION OF CLUSTER

Here the CH is selected as per their weight value. It is calculated dynamically. The weight values of the nodes in the network is estimated on certain parameters such as node degree, virtual battery power, neighbor's average distance and average speed[33][34][35]. Weight values is used because, when in a network any CH has compromised or dead the other nodes associated with that CH will be isolated. As so avoid this scenario nodes try to associate with the other nodes in the nearby region having high configuration. In such case the node having less average speed and high virtual battery power takes the power as CH. [33][34][35]. Generally nodes having high configuration is elected as CH.

IV. DYNAMIC KEY MANAGEMENT

A. COST FUNCTION

For the purpose of security keys are generated dynamically. This key is be generated by the source node and same on destination node without exchanging any keying information. Dynamic key is generated by using source and destination identifiable dynamic parameters inside network. It is used for authentication also. There are various parameters among which virtual battery power plays a major role. CH has a member table in which it records the details of each member in the network along with its ID, NL, ND and virtual battery power. Based on these parameters CCV is computed for each SN.In the architecture, the location is estimated based on Dynamic Reference Localization[36]. All these three parameters are dynamic in nature and the value of CCV depends on them.

B. DYNAMIC KEY GENERATION AND ENCODING

Key is generated based on the transient value of CCV. When node transmits data it uses its virtual battery power for generating key. That node transmits and encrypts the data to its associated CH. At the receiver end the CH generates the same key for decrypting the data.CH has to use the size of data received and previous virtual battery power. Of the same node. As CH generates the correct key, RC5 mechanism is referred. The key to RC5 is generated dynamically. When the next CH along the path to sink receives the packet, it generates the *KD* locally to decode the packet. The source node need to maintain the secured reports and vvirtual battery power for the construction of the next key. This key is the input for RC5 algorithm in the encoding module.

C. KEY UPDATING TECHNIQUE

Key is updated when certain node is added or when a certain node leaves the cluster or when CH leaves the cluster. In these three cases a key i8s updated.

D. AUTHENTICATION TECHNIQUE

For prevention of the misuse of the authenticated nodes or from cheating the authenticated nodes the keys are dynamically changed. HMAC code is generated by using the same key. In this case attacker can not fool the user and not be able to use previous keys.

V. BI-DIRECTIONAL MALICIOUS NODE DETECTION

A Bidirectional malicious node detection mechanism has been included to improve the security. It identifies the malicious node among CH and member nodes. The malicious member nodes are identified by the CHs and the malicious CHs are identified by the BS. For identification a trust based malicious node detection model is used based on hierarchical trust management protocol in FenyeBao at. al.[37]. This works on the major issues like when the the node is compromised and used as malicious nodes to disrupt the network service.

Algorithm: Key Updating Process
If N_i leaves a cluster then
    N_i notifies CH
    CH authorizes N_i
    CH re-computes CCV of its members
else if N_i joins cluster then
    N_i sends join request to CH
    CH sends acknowledgement to N_i
    N_i informs CH of its V_{BP} NL and ND
    CH authenticates N_i
else if CH leaves cluster then
    CH notifies its cluster members
    Re-election of CH takes place
    New CH re-computes CCV of its cluster members
end if

A. TRUST ESTIMATION

Trust estimation have three components truthfulness, number of transmission attempts, direct interactions.

B. MALICIOUS NODE DETECTION ALGORITHMS

Two algorithm were implemented for the purpose. Malicious CH detection and Malicious node detection.

a. DETECTION OF MALICIOUS NODE

CH looks the trust value of data transmitted by its CM and find whether CM is malicious or not. Which can be checked considering two cases. First the value of data transmission trust value is less than threshold and vice-versa. In first case found true then CM will be marked as ML and in second case the node will be considered as trusted. When the malicious node is detected the CH broadcasts the message to its members which includes the identity and dynamic key in it. When it gets message it disconnect the its link and key refreshment is performed associated with that node. By this method malicious node I eliminated but it CH may be malicious.

ISSN: 2394-4404

b. DETECTION OF MALICIOUS CH

Again two cases are considered BS computes $T_{BSj\ (t)}$ of CH and is verified with TT_{BS}. In first case $T_{BSj\ (t)}$ greater than TT_{BS}, then CH will be a trusted node while in vice-versa CH is marked as malicious node. When CH is found malicious BS broadcasts the CHIC to all cluster members. The transmitted invalidation command when recognized by $CM_i$and revealed by CH_i, the CM_i terminates the data transmission and performs CH reelection.

c. SECURITY ANALYSIS

Bi-directional malicious node detection and malicious CH detection ia applied by which malicious nodes are identified and isolated. Three components were used for that.

VI. SCREEN SHOTS AND RESULTS

A. CLIENT SIDE

Figure 1.1: Login window

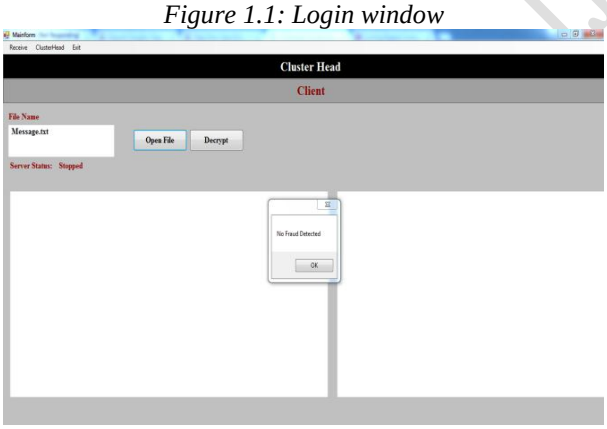

Figure 1.2: After Detection Mechanism

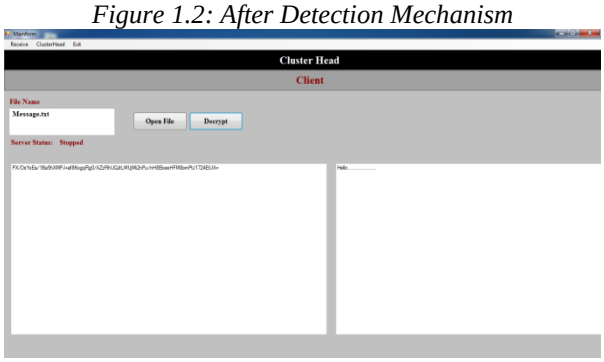

Figure 1.3: Client Side Decryption

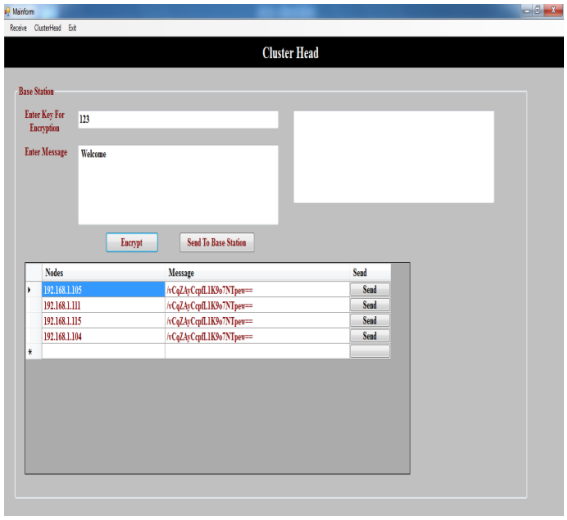

Figure 1.4: Encryption

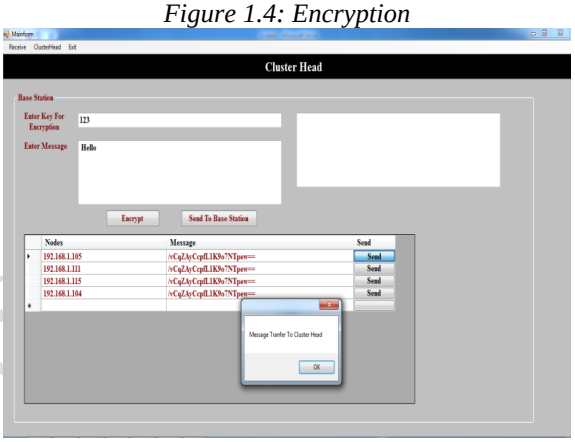

Figure 1.5: Message To CH

B. SERVER SIDE

Figure 2.1: Login Window

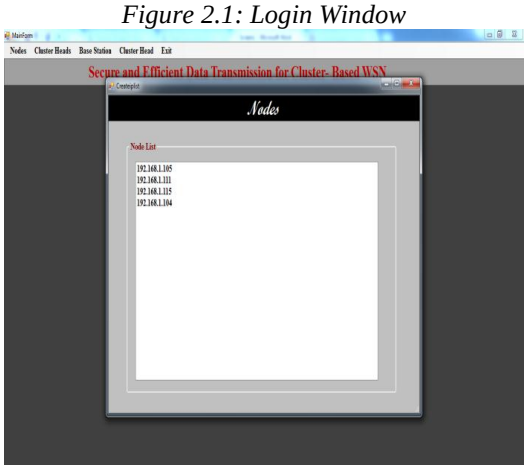

Figure 2.2: nodes

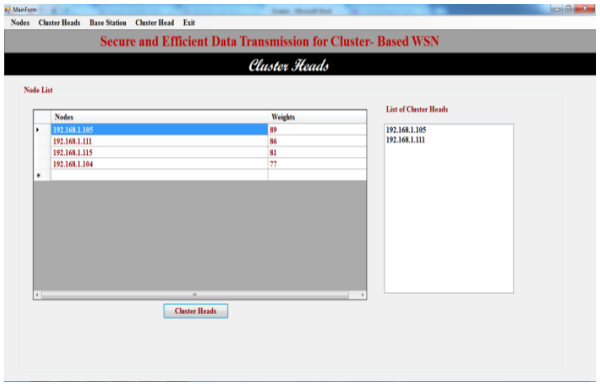

Figure 2.3: Cluster Head

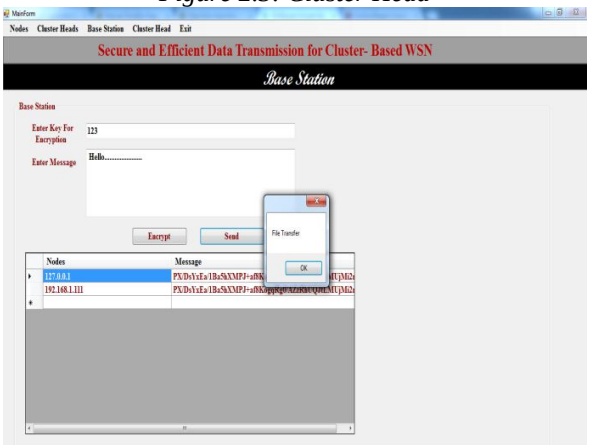

Figure 2.4: File Transfer

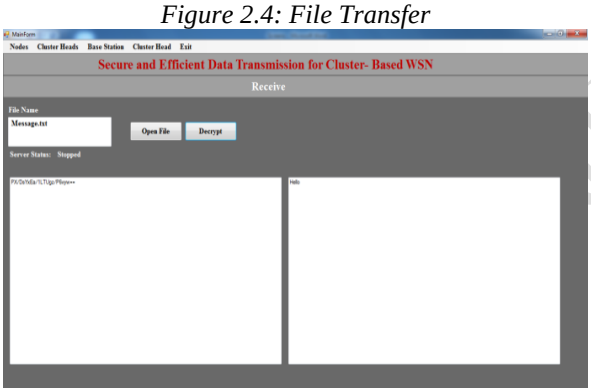

Figure 2.5: File Received

VII. RESULTS

Fig. 1 shows the comparison of alive nodes' number, in which the proposed protocols versus proposed. The results demonstrate that the proposed protocols consume energy faster than SET IBOOS protocol because of the communication and computational overhead for security of either IBOOS process.

Time	SET-IBOOS	Proposed
0.5	6	7
1	5	6
1.5	4	5
2	3	5
2.5	3	4
3	2	4

Table 1

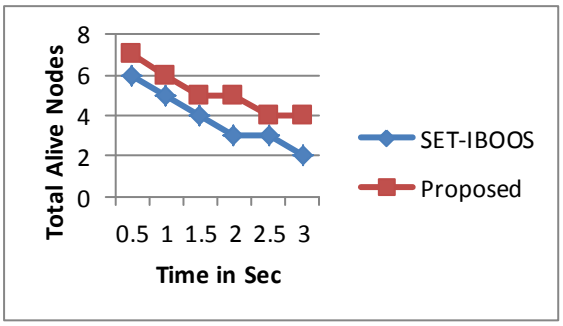

Figure 2.6: Comparison of the number of alive nodes in different protocols

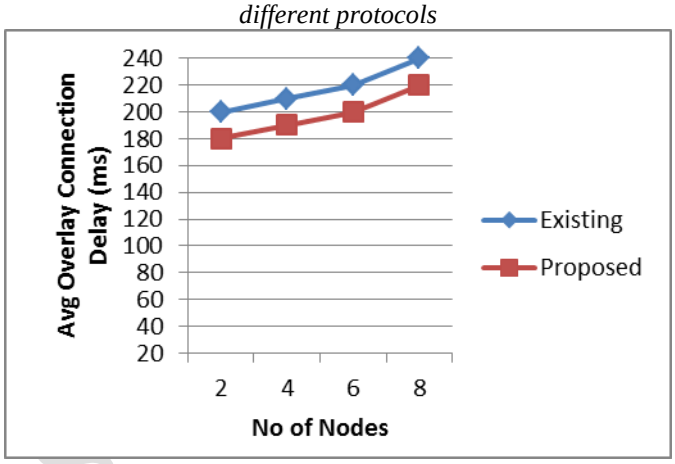

Figure 2.7: Comparison of Existing And Proposed Mechanisms

Nodes	Existing System	Proposed System
2	200	180
4	210	190
6	220	200
8	240	220

Table 2

VIII. CONCLUSION

A secure mobility aware dynamic keying technique for authentication in WSN is proposed in this paper. Cluster head is elected based on its weight value and various parameters are taken into consideration for that purpose. A bi-directional malicious node and malicious cluster head detection mechanism is also employed. Authenticated key management mechanisms is applied in case when a new node wishes to join or a existing node tends to leave the network. Cluster member nodes performs the election of the cluster head. This method has better results in providing security in H-WS.

REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, Wireless Sensor Network Technologies for the Information Explosion Era, Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2] Y. Wang, G. Attebury, and B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE

Comm. Surveys & Tutorials, vol. 8, no. 2, pp. 2-23, Second Quarter 2006.
[3] Patrick Traynor et al., "Efficient hybrid security mechanisms for heterogeneous sensor networks," IEEE Transactions on Mobile Computing, vol. 6, pp. 663-677, 2007.
[4] Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang, and Dharma P Agrawal, "Intrusion detection in homogeneous and heterogeneous wireless sensor networks," IEEE Transactions on Mobile Computing, vol. 7, no. 6, pp. 698–711, 2008.
[5] OssamaYounis and Sonia Fahmy, "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad-hoc Sensor Networks," IEEE Transactions on Mobile Computing, vol. 3, no. 4, pp. 366 – 379, 2004.
[6] Dilip Kumar, Trilok C. Aseri, and R. B. Patel,"EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor network," Computer Communications, vol. 32, no. 4, pp. 662–667, 2009.
[7] Elbhiri. B, Saadane. R, and Aboutajdine. D, "Stochastic Distributed Energy-Efficient Clustering (SDEEC) for Heterogeneous Wireless Sensor Networks," ICGST International Journal on Computer Network and Internet Research, CNIR, vol. 9, no. 2, pp. 11-17, 2009.
[8] Song MAO and Cheng-lin ZHAO, "Unequal clustering algorithm for WSN based on fuzzy logic and improved ACO," The Journal of China Universities of Posts and Telecommunications, vol. 18, no. 6, pp. 89-97, 2011.
[9] DusitNiyato, EkramHossain, and Sergio Camorlinga, "Remote Patient monitoring service using heterogeneous wireless access networks: Architecture and optimization," IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, pp. 412-423, 2009.
[10] Eleni Klaoudatou, Elisavet Konstantinou, and Georgios Kambourakis, "A survey on cluster- based group key agreement protocols for WSNs," IEEE Communications Surveys Tutorials, vol. 13, no. 3, pp. 429– 442, 2011.
[11] Kirusnapillai Selvarajah, Carl Shooter, Luca Liotti, and Alan Tully, "Heterogeneous wireless sensor network for transportation system applications," International Journal of Vehicular Technology, vol. 853948, pp. 14 Pages, 2011.
[12] Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz, "Security issues in wireless sensor networks," International Journal of Communications Letters, vol. 2, no. 1, p. 106–115, 2008.
[13] AylinAksu, Prashant Krishnamurthy, David Tipper, and OzgurErcetin, "On Security and Reliability Using Cooperative Transmissions in Sensor Networks," Mobile Networks and Applications, vol. 17, no. 4, pp. 526-542, 2012.
[14] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Comm., vol. 1, no. 4, pp. 660- s670, Oct. 2002.
[15] Fei Hu, WaqaasSiddiqui, and Krishna Sankar, "Scalable Security in Wireless Sensor and Actuator Networks (WSANs): Integration Re-keying with Routing," Computer Networks, vol. 51, no.1, pp. 285-308, 2007.
[16] Yixin Jiang, Chuang Lin, Minghui Shi, and Xuemin (Sherman) Shen, "Self-healing group key distribution with time-limited node revocation for wireless sensor networks," Ad Hoc Networks vol. 5, no. 1, pp. 14-23, 2007.
[17] Ashraf Wadaa, Stephan Olariu, Larry Wilson, and Mohamed Eltoweissy, "Scalable cryptographic key management in wireless sensor networks," in Int. Conf. on Distributed Computing Systems Workshops, 2004, pp. 796–802.
[18] A. Manjeshwar, Q.-A. Zeng, and D.P. Agrawal, "An Analytical Model for Information Retrieval in Wireless Sensor Networks Using Enhanced APTEEN Protocol," IEEE Trans. Parallel & Distributed Systems, vol. 13, no. 12, pp. 1290-1302, Dec. 2002.
[19] S. Yi et al., "PEACH: Power-Efficient and Adaptive Clustering Hierarchy Protocol for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/15, pp. 2842-2852, 2007.
[20] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28,2012.
[21] L.B. Oliveira et al., "SecLEACH-On the Security of Clustered Sensor Networks," Signal Processing, vol. 87, pp. 2882-2895, 2007.
[22] P. Banerjee, D. Jacobson, and S. Lahiri, "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks," Proc. IEEE Sixth Int'l Symp. Network Computing and Applications (NCA), pp. 145-152, 2007.
[23] K. Zhang, C. Wang, and C. Wang, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using Group Key Management," Proc. Fourth Int'l Conf. Wireless Comm., Networking and Mobile Computing (WiCOM), pp. 1-5, 2008.
[24] S. Sharma and S.K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," Proc. Int'l Conf. Comm., Computing & Security (ICCCS), pp. 146-151, 2011.
[25] G. Gaubatz et al., "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. Workshops (PerCom), pp. 146-150, 2005.
[26] W. Diffie and M. Hellman, "New Directions in Cryptography," IEEE Trans. Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.
[27] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," Proc. Advances in Cryptology (CRYPTO), pp. 47-53, 1985.
[28] D.W. Carman, "New Directions in Sensor Network Key Management," Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.
[29] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.
[30] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.

[31] J. Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l J. Information Security, vol. 9, no. 4, pp. 287-296, 2010.
[32] Thiruppathy Kesavan V and Radhakrishnan S, "Cluster based dynamic keying technique for authentication in wireless sensor networks," in Mobile Communication and Power Engineering.: Springer, 2013, vol. 296, pp. 1-8.
[33] Rico Radeke and Stefan Türk, "Node Degree based Improved Hop Count weighted Centroid Localization Algorithm," in Int. Conf. on Communication in Distributed Systems (KiVS'11), Kiel, Germany, 2011, pp. 194-199. Sung-Chan Choi, Seong-Lyong Gong, and Jang-Won Lee, "An average velocity-based routing protocol with low end-to-end delay for wireless sensor networks," IEEE Communications letters, vol. 13, no. 8, pp. 621–623, August 2009.
[34] ArifSelcukUluagac, Raheem A Beyah, Yingshu Li, and John A Copeland, "VEBEK: Virtual energy- based encryption and keying for wireless sensor networks," IEEE Transactions on Mobil Computing, vol. 9, no. 7, pp. 994– 1007, 2010.
[35] Sung-Chan Choi, Seong-Lyong Gong, and Jang- Won Lee, "An average velocity-based routing protocol with low end-to-end delay for wireless sensor networks," IEEE Communications letters, vol. 13, no. 8, pp. 621–623, August 2009.
[36] Yi-Ling Hsieh and Kuochen Wang, "Efficient localization in mobile wireless sensor networks," in IEEE Int. Conf. on Sensor Networks, Ubiquitous, and Trustworthy Computing, (SUTC'06), vol. 1, 2006, pp. 292–297.
[37] FenyeBao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Transactions on Network and Service Management, vol. 9, no. 2, pp. 169-183, June 2012.