ENSURING SECURITY IN AN ENERGY EFFICIENT LEACH

Prapulla S B[1], Dr. ShobhaG[2], Dr. Tanuja T C[3]

[1,2] R.V.College of Engineering, Department of Computer Science and Engineering, Bangalore, (India)

[3]Vishweshwaraiah Technological University, VLSI Design and Embedded Systems, PG Studies, Belgaum, (India)

ABSTRACT

Wireless Sensor networks have immense applications in areas with no fixed infrastructure. Sensor nodes possess limited computing capability and energy resource. The optimal use of resources is crucial in resource-constrained wireless sensor networks to increase the network lifetime. One of the most successful routing protocols that increase network life time is LEACH- Low Energy Adaptive Clustering Hierarchy. The energy issue has been tackled in this paper by using a variant of LEACH which takes into account the residual energy of all the nodes during cluster head election. This increases the life time of the network. Besides prolonging the network lifetime, fulfilling security requirements is vital as wireless sensor networks are generally applied in crucial applications where security plays an important role. To enforce security, the paper has implemented Secure and Efficient data Transmission - Identity Based Online/Offline digital Signature scheme and has enhanced it for inter-cluster movement of nodes. The data from sensor nodes has been encrypted using Advanced Encryption Standard algorithm.An attempt has been made to increase data efficiency by increasing network lifetime. The experimental result by considering the residual energy of nodes for threshold calculation provides high data efficiency.

I INTRODUCTION

In recent decades a lot of technological achievements have taken place in the field of wireless networks, which are now widely deployed and highly developed. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors which are capable of monitoring physical or environmental conditions, such as temperature, sound, pressure, etc. and then passing their data through the cluster head to a trusted authority which is a base station (BS). Sensor network contain battery powered wireless devices. They have limited storage, processing, communication and sensing capabilities [1][2][3][4].

WSNs are applied in many fields including military[5][6], intelligent buildings, intelligent transportation, smart home systems and environmental monitoring[7]. The routing algorithms which have been designed for traditional wireless networks may not be directly applicable to WSNs. The energy efficient routing protocols in

WSN can be classified into three categories: data centric protocols[8][9], location based protocols[9] and hierarchical protocols[10][11][12].

The availability of resources is limited in a wireless sensor networks. There should be optimal use of resources to increase network lifetime. Another aspect of equal importance is providing security which has great number of challenges because of many reasons like broadcast nature of wireless communication, limited resources, unattended nature of application and being prone to physical attacks[13][14][15]. The most successful approach that organizes the network into a connected hierarchy is clustering. Clustering maximizes node lifetime and reduces bandwidth consumption by using collaboration among sensor nodes[16]. In this scheme, each cluster region should have a cluster head (CH). Cluster head acts as the coordinator node and performs the special tasks such as data aggregation from all sensor nodes under it, before sending it to BS.A base station is a fixed communications location which is responsible for collecting information from the cluster head and acts as a Trusted Authority(TA)[17]. The node with the highest amount of energy is elected as cluster head(CH)[18].

Several clustering algorithms have been proposed in the last decade. LEACH(Low Energy Adaptive Clustering Hierarchy) is one such algorithm. LEACH also provides efficient routing by using cluster formation. It uses the mechanism of CH rotation by random selection of CH for each round. Each node carries an equal probability of becoming the CH. The advantage of LEACH algorithm is that it balances energy consumption and therefore leads to increase in the network lifetime. Overcoming the various limitations of LEACH, other LEACH based protocols have been proposed such as Hierarchical-LEACH,LEACH-Fixed, LEACH-Centralized, Energy-LEACH[19].

Addition of security to LEACH like protocol is demanding due to its random dynamic nature. To achieve this, encryption and authentication should be used. Most of the existing wireless sensor network security protocols make use of variations of symmetric key, MAC[20] and pre-distributed key[21][22] schemes to provide confidentiality, integrity and authentication of every node.

This paper maximizes network lifetime by selecting the CH based on residual energy of sensor nodes. This paper also tackles and enhances various security issues like confidentiality and authentication. To maintain confidentiality, it uses Advanced Encryption Standard(AES) which provides high security with low energy consumption[23]. To provide authentication, it implements digital signatures by using identity information of the sensor nodes.

1.1 Literature Survey

Clustering is considered as one of the techniques prolonging the lifetime of WSN especially in a Cluster-based WSN (CWSN), since there is a cluster head node for every cluster. The function of the Cluster Head(CH)is to aggregate the data collected by each and every leaf node and send the aggregated data to the base station (BS). The LEACH (Low-Energy Adaptive Clustering Hierarchy) protocol presented by Heinzelman et.al. [24][25] isa widely accepted and popular one[5]. It balances and reduces the total energy consumption of CWSN. LEACH randomly rotates cluster heads among all sensor nodes so that the energy of a single node is notdrained as a CH.

There are many limitations of LEACH such as there is no mechanism for uniform distribution of cluster heads and does not consider energy of the nodes during CH selection process. On the basis of the LEACH, a number of protocols have been presented such as APTEEN, PEACH, LEACH-F, LEACH-C, E-LEACH, V-LEACH, H-LEACH which use similar concepts of LEACH[18][24].Ensuring security in LEACH based protocol is challenging as the network's cluster and data links are rearranged dynamically, randomly and periodically[24]. Some secure data transmission protocol based on LEACH have been proposed in recent years like SecLEACH[24][26], GS-LEACH[27] and RLEACH[28]. Most of the existing secure protocols use symmetric key management for security.

This suffers from a problem called orphan node problem. The problem occurs when a node does not share a secret key with others. Thus the secret key is not present in the preloaded key ring. Also the key ring may not be large enough to store the keys of all nodes in a large network. In such cases, orphan nodes elect themselves as CHs. If this continues, then there will be more number of CHs which leads to higher consumptions of energy. In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman proposed the RSA algorithm at MIT. This exploits the difficulty of factoring large numbers to ensure security. This algorithm also provides the authorization using the digital signatures. In 1984, Adi Shamir proposed the ID-based cryptography system[29][30][31]. This was an extension of RSA[32]. In this, identity information is used to create digital signature. The identity information in a WSN can be a name, node number or the IP address.The Identity Based digital Signature (IBS) scheme has been proposed taking into account difficulty of factoring integer from identity based cryptography (IBC)[24].IBOOS scheme has been proposed aiming to reduce the computation and storage costs.

The identity based cryptographic schemeshave been recently extended to Wireless Sensor Networks[2][33]. In 2013, Huang Lu, Jie Li, Mohsen Guizani have proposed two protocols SET-IBS and SET-IBOOS for WSN's based on IBS and IBOOS respectively[24].SET-IBOOS is a protocol to authenticate the encrypted sensed data, by applying digital signatures to message packets. It generates offline signature at the cluster head and online signature at sensor nodes. The SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs[24].

1.2 Problem Statement

The problem of the existing system using LEACH protocol is that it does not take into account the residual energy of the nodes during cluster head election. The variants of LEACH proposed like F-LEACH, C-LEACH, V-LEACH also suffer from the same problem leading to reduced network lifetime. Another major issue is addressing security as WSNs are used in critical tasks[34][35][36].

Several secure LEACH protocols have been proposed like SecLEACH[24], GS-LEACH[27], S-LEACH[37][38] which use symmetric key management for security resulting in orphan node problem due to limited key ring size. This leads to additional cluster head selection and decreases the energy of the nodes which results in overall network lifetime reduction.

1.3 Proposed System

To overcome these problems, the paper implements a variant of LEACH which takes into account the residual energy of nodes during threshold calculation. The security is enhanced by using digital signatures using identity information.

II SYSTEM DESIGN

2.1 Design Considerations

This section addresses the various issues that need to be discussed or resolved before attempting to devise a complete design solution.

2.1.1 General Constraints

The major constraints of the paper have been listed as follows:

- The cluster head election must be done in reasonable amount of time and the cluster head election must be rotated based on energy.
- The program must be suitably robust to handle data from each node and to handle multiple clusters.
- The system must have NetBeans IDE 6.9.1 or higher with JDK 1.6 or higher installed.
- The operating system in use must be Windows 7(or any equivalent) or higher

2.2 Architectural Strategies

This section describes the design decisions and strategies that will affect the overall organization of the system and the higher-level structures. These strategies will provide insight into the key abstractions and mechanisms used in the system architecture.

2.2.1 Programming Language

The efficiency and future development of the paper is based on programming language chosen. As such, Java has been chosen as the programming language to be used.

2.3 System Architecture

The architectural design process establishes a basic framework for a system which includes identifying the major components of the system and communications between these components [45].

The figure 2.1 shows the blocks required each block represents a module that is to be developed. Each module is a function that is to be performed and is itself comprised of smaller tasks.

2.3.1 System Parameter Initialization

The system parameter initialization is done by the base station. It generates distinctive node IDs and keys which will be used for encryption and decryption. These are generated for every node in the network. It is then distributed to the respective nodes. The base station also receives the encrypted data from all the cluster heads. The base station verifies the signature of a node when it moves from one cluster to the other.

2.3.2 Cluster Formation

A node generating random value greater than the threshold elects itself as the cluster head and advertises itself to each of the nodes in its cluster. In case of a situation where two or more nodes are capable of being a cluster head, the node which first advertises itself will be elected as the cluster head. The sensor nodes in a cluster are at a distance of one hop from the cluster head. The cluster head is also involved in the generation of offline signature for each of the nodes in its cluster.

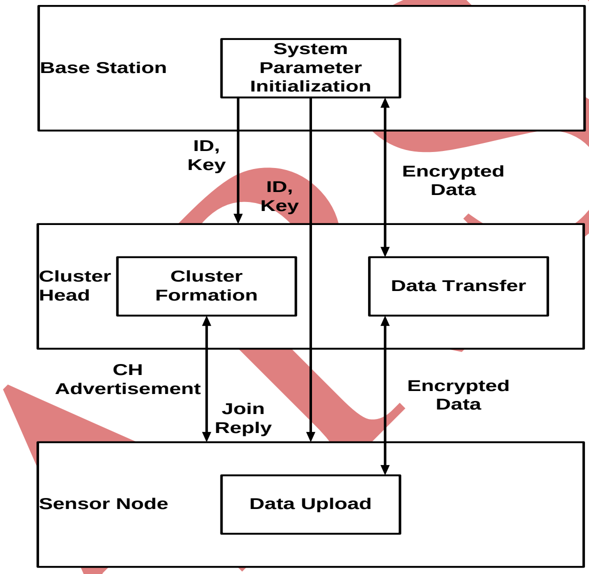

Figure 2.1 System Architecture

2.3.3 Data Upload Process at Sensor Nodes

The sensor node sends data during the steady phase of every round of LEACH protocol. The data upload process is involved in generation of online signature generation from the offline signature generated by the cluster head. The online signature is sent along with the encrypted data to the cluster head for authentication.

2.3.4 Data Transfer Process at Cluster Head

The encrypted data from each sensor node is received and the validity of signature is checked and it is forwarded to the base station by the cluster head. A fresh signature is generated in each and every round of LEACH protocol.

III DETAILED DESIGN

Detailed Design is a phase wherein further details and algorithmic design of each of the modules is specified.

This section presents the following:

- Structure Chart
- Functional Description of modules

3.1 Structure Chart

A Structure Chart depicts the control flow among the units in a system by making use of control and data flags. The Structure Chart explains the identified units and the interaction between the units.

There are 4 main modules in this paper:

1. System Parameter Initialization
2. Cluster Head Selection
3. Data Transfer Process
4. Inter Cluster Movement

The sequence of flow and control of each module / sub-module is shown in figure 5.1. This is a structured chart that represents all the modules and the data that flows in them.

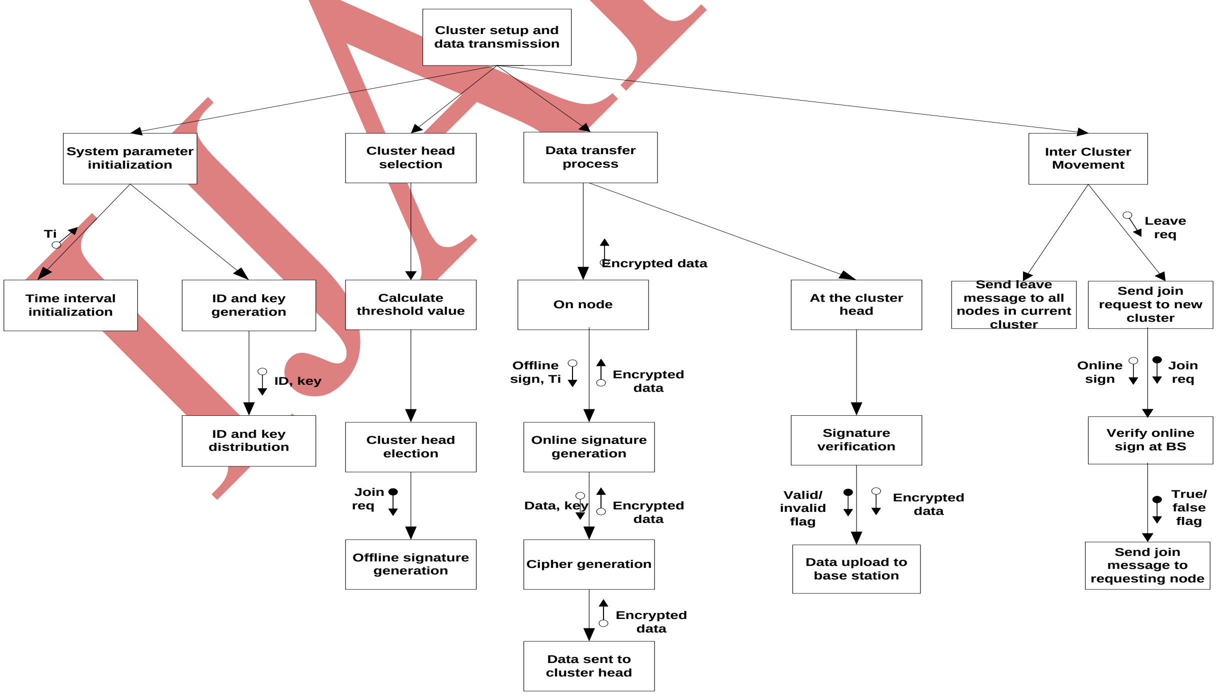

Figure 3.1 Structure Chart

3.2 Functional Description of Modules

This section contains a detailed description of software components, low-level components and other sub components of the paper.

3.2.1 System Parameter Initialization module

This section contains some information on the functionality and some software component attributes of the System Parameter Initialization Module.

Purpose: The purpose of this module is to define the time interval for the rounds of LEACH protocol, namely setup and steady and generation of ID and Key for each and every node.

Functionality: The functionality of this module is to generate and distribute IDs to each node belonging to cluster and generate pair wise key for encryption/decryption.

3.2.2 Cluster Head Selection module

This section contains some information on the functionality and some software component attributes of the Cluster Head Selection Module.

Purpose: The purpose of this module is to select the cluster head based on random number greater then calculated threshold value.

Functionality: The functionality of this module is cluster head selection process and generation of offline signature.

3.2.3 Data Upload Module at Nodes

This section contains some information on the functionality and some software component attributes of the Data Upload Module at Nodes.

Purpose: The purpose of this module is to read the data and send encrypted data to the cluster head.

Functionality: The functionality of this module is to generate cipher text and generate online signature. It is also involved in sending the encrypted data and signature to the cluster head.

3.2.4 Data Upload Module at Cluster Head

This section contains some information on the functionality and some software component attributes of the Data Upload Module at Cluster Head.

Purpose: The purpose of this module is to receive data from the sensor nodes and forward it to the base station.

Functionality: The functionality of this module is to receive the data packets from the sensor nodes, verify the online signature and forward the data to the base station.

3.2.5 Inter Cluster Movement Module

This section contains some information on the functionality and some software component attributes of the Inter Cluster Movement Module.

Purpose: The purpose of this module is to allow sensor nodes to move from one cluster to another within same network.

Functionality: The functionality of this module is to verify the online signature of the sensor nodes at the base station and allow it to join new cluster.

This section focused on the detailed design of all the modules. It covered structure chart. It explained the key modules involved in the paper.

IV EXPERIMENTAL ANALYSIS AND RESULTS

This chapter lists the results of the paper and the inferences to be made from the experimental results. The evaluation metrics have been listed and the results have been accordingly quantified. The results indicate the general performance trend of the paper developed.

4.1 Evaluation Metric

The main metric to evaluate performance is the number of rounds in which data is received at the base station from the sensor nodes. Higher efficiency is achieved if data is sent in every round.

Another important metric is the number of times a node is elected as a cluster head. This metric shows the fair distribution of cluster heads among all the sensor nodes.

4.2 Performance Analysis

The figure 4.1 shows the number of rounds in which data was received at the base station when the number of rounds was 24. The graph shows the mean value of data round taken out of 3 trials. The system achieves high performance when the cluster size is 3 and 4. The data sent by the sensor nodes is received by the base station in most of the rounds.

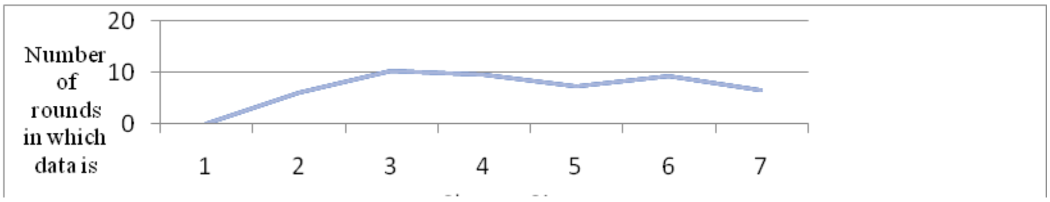

Figure 4.1 Number of rounds in which data is sent for various cluster sizes

The paper has implemented energy-efficient LEACH, which according to simulation results carried out in [28] is 20% more efficient than LEACH. The SET-IBOOS protocol has better performance than existing secure protocols for CWSNs[24]. Since, actual energy consumed cannot be measured in laptops, the results of [24] has been shown in figure 4.2.

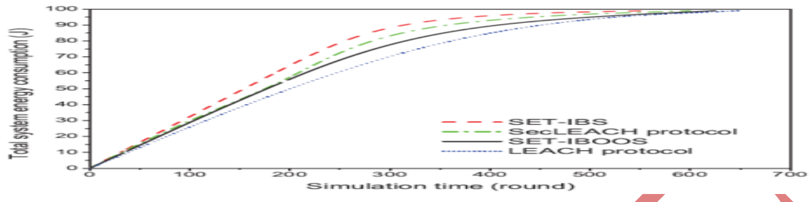

Figure 4.2 Comparison of energy consumption in different protocols[24]

The figure 4.3 shows the number of times a node has become the cluster head for cluster size 2. The distribution of cluster heads among sensor nodes is fair in all the rounds when the cluster size varies from 2 to 5. There is unfair distribution of cluster heads among the sensor nodes when the cluster size is 6 and above.

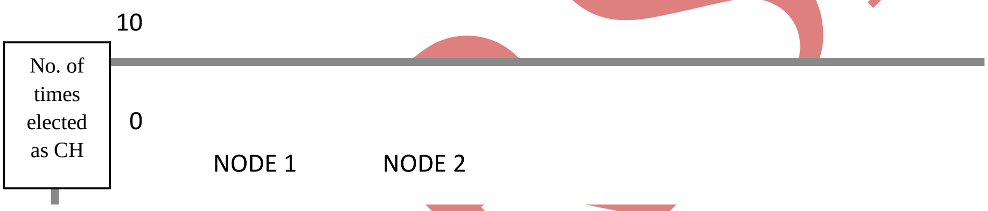

Figure 4.3 Distribution of cluster heads (cluster size = 2)

The figure 4.4 shows the number of times a node has become the cluster head for cluster size=3.

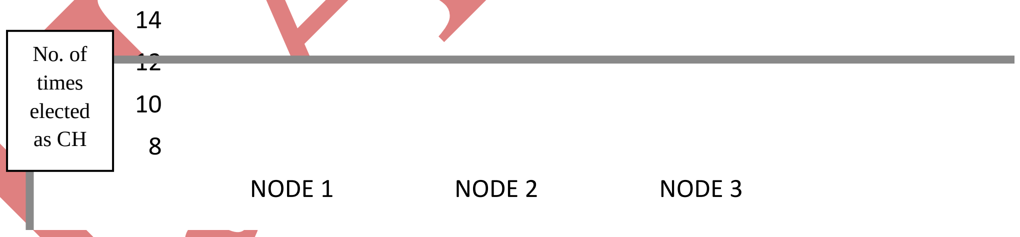

Figure 4.4 Distribution of cluster heads (cluster size = 3)

The figure 4.5 shows the number of times a node has become the cluster head for cluster size 4.

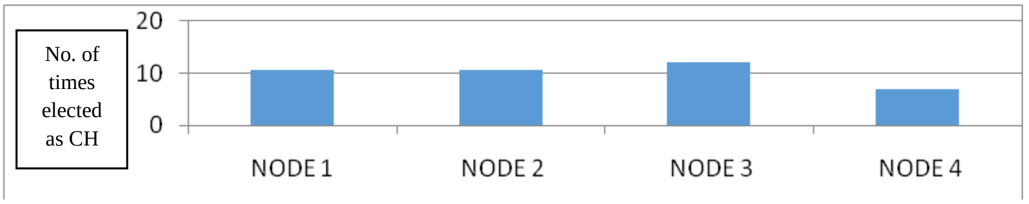

Figure 4.5 Distribution of cluster heads (cluster size = 4)

The figure 4.6 shows the number of times a node has become the cluster head for cluster size 5.

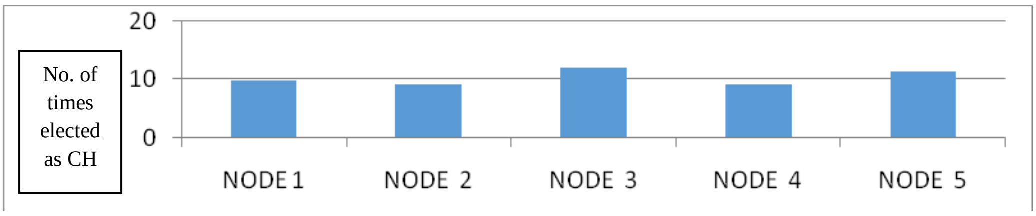

Figure 4.6 Distribution of cluster heads (cluster size = 5)

The figure 4.7 shows the number of times a node has become the cluster head for cluster size 6.

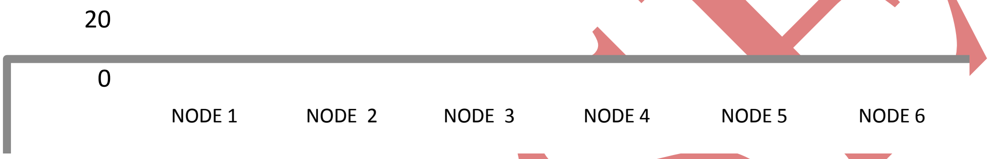

Figure 4.7 Distribution of cluster heads (cluster size = 6)

4.3 Inference from the Result

It is clear from the experimental analysis that the paper developed has an optimal cluster size of either 3 or 4 to achieve fair distribution of cluster heads among the nodes and achieve high throughput. According to work in [51], the optimal cluster size for a small network consisting of 256 nodes, the optimal cluster size is 4. The achieved optimal cluster size is comparable to this result. For nodes greater than 5, high performance can be achieved by having multiple clusters.

V CONCLUSION

The paper addresses the important issue of ensuring security in an otherwise energy constrained wireless sensor network. In LEACH – one of the most successful clustering protocol, a node with less amount of energy has the same probability of becoming a cluster as that of a node with high energy. This paper aims at overcoming this shortcoming by taking into consideration the residual energy of the nodes during cluster head election.The work enhances security which is very crucial in hostile environments such as battlefield scenarios in WSNs. This is achieved by authentication of nodes by making use of digital signatures. The paper maintains data confidentiality by providing encryption using AES algorithm. The paper also enhances SET-IBOOS protocol forinter-cluster movement of nodes.

5.1 Future Work

- The inter cluster movement module can be enhanced for routing through routes of shorter distances via different cluster head.

- Cluster head selection module can be enhanced to avoid election of multiple cluster heads.
- This can be extended for real world application using actual sensors.
- Many other strong encryption algorithms can be used alternately.
- The paper can be enhanced to measure the actual energy of nodes and use this for better threshold calculation.

REFERENCES

[1] Mehta, R., Pandey, A., and Kapadia, P., “Reforming Clusters Using C-LEACH in Wireless Sensor Networks”, *International Conference on Computer Communication and Informatics*, Coimbatore, India, 10-12 Jan 2012, pp.1-4.

[2]Li, F., Di Zhong, and Takagi, T., ” Practical Identity-Based Signature for Wireless Sensor Networks”, *IEEE Wireless Communications Letters*, Vol.1, (6),10 December 2012, pp 637-640.

[3] Akkaya K., and Younis M., "A Survey on Routing Protocols for Wireless Sensor Networks", *Science Direct*,Vol. 3,(3), May 2005, pp. 325-349.

[4]Akyildiz, I.F., Weilian Su, SankaraSubramaniam, Y., and Cayirci, E., "Wireless Sensor Networks: A Survey", *IEEE Communications Magazine*, Vol. 40,(8), August 2002, pp. 102-114.

[5] ZhiqiangRuan,Qiaoliang Li, Sujun Li.” A Secure Routing Protocol for Clustered Sensor Networks”, *International Conference on Wireless Communications Networking and Mobile Computing*, Dalian, China, 12-14 October 2008, pp. 1-4.

[6] Yong Wang, Attebury, G., and Ramamurthy, B., “A Survey of Security Issues in Wireless Sensor Networks”, *IEEE Communication Surveys and Tutorials*, Vol. 8, (2), 2006, pp. 2-23.

[7] Ying Li, LiPing Du, GuiFen Zhao, FeiDuan, “Research on Lightweight Digital Signature Scheme in Wireless Sensor Network”, *2nd International Conference on Computer Science and Network Technology*, Changchun, 29-31 December 2012, pp.1154-1157.

[8] Li-Qing Guo, Yi Xie, Chen-Hui Yang, Zheng-Wei Jing, ”Improvement On Leach By Combining Adaptive Cluster Head Election And Two-Hop Transmission”, *Proceedings of the Ninth International Conference on Machine Learning and Cybernetics*,Qingdao, China, 11-14 July 2010, pp. 1678-1683.

[9] K. Akkaya and M. Younis, "A survey on routing protocols for wireless sensor networks", *Elsevier Ad Hoc Networks*, Vol. 3, (3), May 2005, pp. 325-349.

[10] Xu D., and Zhang H., "Improved Algorithm of LEACH Protocol Introducing Residual Energy", *Computer Engineering and Applications*, Vol. 45,(28), 2009, pp. 115-119.

[11] Muruganathan S.D., Ma, D.C.F., Bhasin, R.I., and Fapojuwo, A., "A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks", *IEEE Radio Communications*, Vol. 43, (3), March 2005, pp. 8-13.

[12] Thein, M.C.M., and Thein, T., "An Energy Efficient Cluster -Head Selection for Wireless Sensor Networks", *Proceedings ofInternational Conference on Intelligent Systems Modeling and Simulation*, Liverpool, UK, 27-29 January 2010, pp.287-291.

[13] Boneh D., and Franklin M. K., "Identity-Based Encryption from the Weil Pairing", *21st Annual International Cryptology Conference*, Santa Barbara, California, USA, 19-23 August 2001, pp. 213-229.

[14] Boneh D., Gentry C., Lynn B., and Shacham H., "Aggregate and Verificably Encrypted Signatures from Bilinear Maps", *International Conference on the Theory Applications of Cryptographic Techniques*, Warsaw, Poland, 4-8 May 2003, pp. 416-432.

[15] Micali S., Ohta K., and Reyzin L., "Accountable-Subgroup Multisignatures", *ACM Conference on Computer and Communications Security*, New York, USA,2001, pp. 245-254.

[16] Pradeepa K., Anne W. R., and Duraisamy S., "Design and Implementation Issues of Clustering in Wireless Sensor Networks", *International Journal of Computer Applications*, Vol. 47,(11), 2012.

[17] Li, F., Di Zhong, and Takagi, T., "Practical Identity-Based Signature for Wireless Sensor Networks", IEEE Wireless Communications Letters, Vol. 1, (6), 10 December 2012, pp.673-640.

[18] Babaee, E., Zareei, S., and Salleh, R., "Best Path Cluster-based Routing Protocol for Wireless Sensor Networks", *UKSim 15th International Conference on Computer Modeling and Simulation*, Cambridge, 10-12 April, 2013, pp.663-667.

[19] Sharma, M., and Sharma, K., "An Energy Efficient Extended LEACH (EEE LEACH)", *International Conference on Communication Systems and Network Technologies*, Rajkot,11-13 May 2012, pp. 377-382.

[20] Li Yang, and Moh, M., "Dual Trust Secure Protocol for Cluster-based Wireless Sensor Networks",*AsilomarConference on Signals, Systems and Computers*, Pacific Grove, CA, 6-9 Novemeber 2011, pp 1645-1649.

[21] Di Pietro, R.,Mancini,L.V., and Mei,A., "Random key-assignment for secure Wireless sensor Networks", *In proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks*, New York, USA, March 2003, pp 62-71.

[22] Li Yang, and Moh, M., "Dual Trust Secure Protocol for Cluster-based Wireless Sensor Networks", *Forty Fifth Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, Pacific Grove, CA, 6-9 November 2011, pp.1645-1649.

[23] Modirkhazeni, A., Ithnin, N., and Ibrahim, O., "Secure Multipath Routing Protocols in Wireless Sensor Networks: A Security Survey Analysis", *Second International Conference on Network Applications, Protocols and Services*, Kedah, Malaysia, 22-23 September 2010, pp.228-233.

[24]Huang Lu, Jie Li, and Guizani, M., "Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25,Issue 3, 18 Feb 2013, pp.750-761.

[25]Heinzelman, W.B., Chandrakasan, A.P., and Balakrishnan, H., "An application specific protocol architecture for wireless microsensor networks", *IEEE Transactions on Wireless Communications*, Vol. 1, (4), October 2002, pp.660-670.

[26] Oliveira, L.B., Wong, H.C., Bern, M., Dahab R., A.A.F.Loureiro", SecLeach-Random Key Distribution Solution For Securing Clustered Sensor Networks", *Fifth IEEE International Symposium on Network Computing and Applications*, Cambridge, MA, 24-26 July 2006, pp. 145-154.

[27] Banerjee, P., Jacobson, D., and Lahiri, S.N., "Security and Performance Analysis of a Secure Clustering Protocol for Sensor Networks", *International Symposium on Network Computing and Application*, Cambridge, MA, 12-14 July 2007, pp.145-152.

[28] Ningbo Wang, Hao Zhu, "An Energy Efficient Algorithm Based on LEACH Protocol",*International Conference on Computer Science and Electronics Engineering*,Hangzhou, China,Volume:2, 23-25 March 2012, pp. 339-342.

[29] Xu An Wang, WeidongZhong, Haining Luo," Cryptanalysis of an Efficient Hierarchical Identity Based Signature Scheme in the Standard Model", *International Symposium on Intelligence Information Processing and Trusted Computing*, Huanggang, China, 28-29 October 2010,pp. 619-621.

[30] Wun-She Yap, Swee-HuayHeng, Bok-Min Goi," On the Security of an Identity-Based Aggregate Signature Scheme", *22nd International Conference on Advanced Information Networking and Applications – Workshops*, Okinawa, Japan, 25-28 March 2008,pp. 1523-1528.

[31] Bennian Dou, Hong Zhang, ChungenXu, Mu Han, "Identity-Based Sequential Aggregate Signature from RSA", *Fourth ChinaGrid Annual Conference*,Yantai Shandong, 21-22 August 2009, pp 123-127.

[32] Anand, D., Khemchandani, V., and Sharma, R.K., "Identity-Based Cryptography Techniques and Applications", *5th International Conference on Computational Intelligence and Communication Networks*, Mathura, India,27-29 September 2013, pp.343-348.

[33]Li, F., Di Zhong, and Takagi, T., "Practical Identity-Based Signature for Wireless Sensor Networks", *IEEE Wireless Communications Letters*, Vol. 1,(6), 10 December 2012, pp.673-640.

[34] Shi, E., and Perrig, A., "Designing Secure Sensor Networks," *Wireless Communication Magazine*, Vol. 11, (6), Dec. 2004, pp. 38–43.

[35] Ahmad Salehi, S., Razzaque, M.A., Naraei, P., and Farrokhtala, A., "Security in Wireless Sensor Networks:Issues and Challenges", *Proceeding of the 2013 IEEE International Conference on Space Science and Communication (IconSpace)*, Melaka, Malaysia,1-3 July 2013, pp 356-360.

[36] E. Shi and A. Perrig, "Designing Secure Sensor Networks," *Wireless Communication Magazine*, Vol. 11, Issue 6, December 2004, pp. 38–43.

[37] El-Saadawy, M., and Shaaban, E., "Enhancing S-LEACH Security for Wireless Sensor Networks", *IEEE International Conference on Electro/Information Technology*, Indianapolis, IN, 6-8 May 2012, pp.1-6.

[38] Ferreira A.C., Vilac M.A, Oliveira L.B. , , Habib E., Wong H.C. and Loureiro A. A., "On The Security Of Cluster-Based Communication Protocols For Wireless Sensor Networks",*International conference on Networking, Reunion Island*, France, April 17-21 2005, pp.449-458.

[39] Zhao Jinchao, "Research on Key Predistribution Scheme of Wireless Sensor Networks", *Fifth International Conference onIntelligent Computation Technology and Automation*, Zhangjiajie, Hunan,China, 12-14 January 2012, pp.287-290.

[40] Soni, H., Tripathi, P., and Bhadoria, R.S., "An Investigation on Energy Efficient Routing Protocol for Wireless Sensor Network", *5th International Conference on Computational Intelligence and Communication Networks*, Mathura, India, 27-29 September 2013, pp.141-145.

[41] Taghikhaki, Z., Meratnia, N., and Havinga, P.J.M., "A Reliable and Energy-efficient Chain-cluster Based Routing Protocol for Wireless Sensor Networks", *IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, Melbourne, VIC, 2-5 April 2013, pp.248-253.

[42] Jia Xu, NingJin, Xizhong Lou, Ting Peng, Qian Zhou, and Yanmin Chen , "Improvement of LEACH protocol for WSN", *9th International Conference on Fuzzy Systems and Knowledge Discovery*, Sichuan, China, 29-31 May 2012, pp.2174-2177.

[43] Li-Qing Guo, Yi Xie, Chen-Hui Yang, Zheng-Wei Jing, "Improvement On Leach By Combining Adaptive Cluster Head Election And Two-Hop Transmission",*Proceedings of the Ninth International Conference on Machine Learning and Cybernetics*, Qingdao, China, 11-14 July 2010, pp.1678-1683.

[44] Sharma, S., and Jena, S. K., "A survey on secure hierarchical routing protocols in wireless sensor networks",*Proceedings of International Conference on Communication, Computing and Security*, Odisha, India, February 12-14 2011, pp.146-151.

[45]Ian Sommerville, "Software Engineering", Pearson, 9th Edition, 2011, ISBN: 978-0137035151.

[46]Brian Cole, Robert Eckstein, James Eliott, Marc Loy, David Wood, "Java Swings", O'Rielly and Associates, 2nd Edition, November 2002, ISBN: 9780596004088.

[47] Mansour, I., and Chalhoub, G.,."Evaluation of different cryptographic algorithms on wireless sensor network nodes", *International Conference on Wireless Communications in Unusual and Confined Areas*, ClemontFerrand, France, 28-30 August 2012, pp.1-6.

[48] "Cryptography and Network Security",TataMcgraw Hill Education Private Limited, 2nd Edition, 2011, ISBN: 9780070702080.

[49] Roger S Pressman, "Software Engineering A Practitioners' Approach", Tata Mcgraw Hill Publishers, 7th Edition,2010, ISBN: 9780073375977.

[50] Davis Flanagan, "Java in a Nutshell", O'Reilly and Associates, 5th Edition, 2005, ISBN: 9780596007737.

[51] Förster, Anna, Förster, Alexander, and Murphy, Amy L., "Optimal Cluster Size for Wireless Sensor Networks: An Experimental Analysis", Ad Hoc Networks, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Vol. 28, Springer Berlin, Heidelberg, 2010, pp.49-64.