International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6, August, 2019

Improved Version of Secure Watermarking LEACH: R-Watermarking LEACH

Rekha Rani, Harmaninderjit Singh

Abstract— ***As wireless sensor networks (WSN) deployment are broadly spreading in various fields. Therefore security becomes a vital issue. Most of the researcher's attention is only on utility of sensor network and possibility of sensor network rather than security. In our work we do focus on security for that we consider privacy and integrity the main issues of sensor networks related to security. In WSNs, various schemes have previously introduced by various researchers to manage security, but few algorithm have been considered the privacy and integrity at both sensor nodes cluster member and CH nodes. In our work we have present a secure algorithm to control integrity and privacy at both node level and cluster head level in WSN. In our protocol we have control the integrity by watermarking technique and privacy is managed using encryption technique.***

Keywords— Integrity, Privacy, Cryptography, Watermarking

I. INTRODUCTION

With extending use of internet, sensor computing devices like mobile phones, PDA, computers, servers, PCs, Laptops, etc. Wireless sensor networks are becoming popular. In WSN these computing devices have a small sensor to sense data, actuators is used to check the physical changes of network and wireless communication [1]. Sensor units have limited energy for processing, tiny memory device, and little bandwidth. Sensor network is very easy to establish and have low cost so it is used in various fields of science and technology to watch and handle various activity like military surveillance , analyzing highway traffic, wildlife and ocean pollution, earthquake, fire in forest, water level in sea, safety of buildings, manufacturing machinery performance etc. [2]. In most cases sensor networks are placed in hostile and inaccessible location and sensor units are randomly scattered in network, and attacker could easily interrupt in network, temper the data, and use this data as per their need, therefore security is a difficult task in WSN [3][4][5]. the functioning of wireless networks like attacker may corrupt the services of network or die a particular nodes. Denial-of-Service (DoS), black hole, jamming, sinkhole, wormhole, Sybil and flooding types are some common attacks of these type [6][7]. To avoid these attacks Encryption, Cryptography, authorization, confidentiality, authentication, and data integrity security schemes are used [8].

Revised Manuscript Received on October 30, 2019.

* Correspondence Author

Rekha Rani* , Research scholar Department of Computer Science, Desh Bhagat University , Mandi Gobindgarh (Punjab), India. rekha_nskalra@yahoo.co.in

Harmaninderjit Singh, Assistant professor in Computer Science, Desh Bhagat University , Mandi Gobindgarh (Punjab), India, jeetsinder@gmail.com

Conventional security schemes are suitable for desktop, PDA etc. but not good for sensor devices. For sensor devices various security schemes are proposed by many researchers. We structured the paper as follows. Section 2 discuss about literature survey.
Section 3 presents the different existing security schemes of wireless sensor networks. Section 4 discusses the purposed algorithm R-Watermarking LEACH. Section 5 is the performance evolution. Section 6 discusses the simulation result of purposed scheme based on detection rate. In Section 7 we compare purposed R-Watermarking LEACH protocol with Watermarking LEACH. At last, we conclude our the paper in 8th section.

II. RELATED WORK

Due to small power unit sensor nodes have limited computation power so symmetric cryptographic algorithms are more suitable for wireless sensor network than Asymmetric cryptographic algorithms [9]. But sensor nodes have small size memory and restricted key length so symmetric cryptographic algorithms do compromise with security [10]. To resolve this problem a new secure energy-efficient routing protocol is designed with use of symmetric cryptographic techniques and NOVSF code-hoping algorithm which can be used unaltered, irrespective size of network [11]. Karlof, C., & Wagner, D. research encryption and authentication methods of link layer can provide security against attackers however only cryptography technique is not sufficient thus they introduced some new security goal for routing in WSNs, which show that the process how attacks beside ad-hoc and peer-to-peer networks can be modified into powerful attacks adjacent to WSNs, and two classes introduced for novel attacks against wireless sensor networks, and analyzed the security of wireless sensor network routing protocols [12]. A new secure routing protocol among two building block was presented by A. Perrig, which is utilized for WSNs- SNEP. SNEP provides validation, confidentiality, and originality among nodes and the sink node and µTESLA use for authentic broadcasting [13]. One more protocol ESPDA was introduced to avoid the duplicity of data at the time of transmission from node to CH [14]. SEEM is another routing protocol which is designed for increase the lifespan of sensor network and decrease the transmission with the use of shortest and reliable path, and control the attacks which were come through the long path among nodes and sink node another multipath secure [15]. To provide the security of individual node in provisions of space and power Mukherjee, N. give a dynamic cryptographic scheme. This scheme provides the security from the cryptanalytic attacks to decrease consumption power in whole network [16].

Hierarchical protocol by higher energy level sensors may use for processing and sending the data. And nodes with minimum power are use only for data sensing [17]. Jiliang Zhou gives another integrated algorithm to ensure the verification, privacy, originality and reliability of WSN named BEARP, is use for addressing security issues and lifetime improvement. It provides security and efficiency based on authentication and encryption in three phases [18].

III. EXISTING LEACH BASED SCHEMES

LEACH [19] routing protocol is mainly utilized to enlarge the lifespan of wireless sensor network by save energy. Processing of LEACH routing algorithm is separated in various round, wherever starting of round with a setup state, and end with steady state. LEACH elect cluster-head by randomized rotation to save the power of individual sensor node [19]. Threshold value is used to select a cluster head suggested percentage p1, sensors that weren't elect as a cluster head in earlier 1/p1 rounds produce random number among 0 - 1. Following formula is used to set the tthreshold value.

$$T(ni) = \frac{P1}{1-PX\left(ri \bmod \frac{1}{P1}\right)} \qquad \forall ni \in G \qquad (1)$$

$$T(ni) = 0 \qquad \forall ni \in G \qquad (2)$$

In above formula G is group of sensor nodes those are not acted as a head in very last 1/pi rounds, Pi represent recommended percentage of CH, and here ri is represent recent round. The current cluster head will be cluster head after that 1/p1 round [20]. To begin with, each sensor produces random no. among 0 - 1. In case threshold value is greater than random no., the node makes a cluster head for in progress circle. CH broadcast adv_message for member node. Each node of a cluster keep on their receiver mode to listen the advertised broadcast message of CH. CH schedules the transition and broadcast of each node by TDMA scheduling when the clusters are produced and TDMA schedule set, data broadcast is begin [21]. Various algorithms EE-LEACH [22], MODLEACH [23], APTEEN [24], MIMO [25], NEW LEACH [26] are introduced to provide integrity, confidentiality, energy efficiency, privacy, etc. Encryption schemes like DES, ECC, RSA are normally use in WSN for authentication. Mbarek, B., et. al. focuses on architectural and operational challenges of verification [27]. WSNs may be divided in two types network- proactive and reactive networks. Nitin Mittal, et. al. improve LEACH protocol which use sub cluster head with the CH in cluster to properly consume the energy and enhance network life span [28]. Derived from dynamic key cryptography process which use the WBAODV protocol Edvinoe Christina, et.al. have introduced a new protocol named AODV. This protocol is a weight base protocol, in which load of way is conform based on sensor nodes speed, Bandwidth and the level of power unit. This algorithm provides better security because it has, high Throughput, fewer amounts of Energy consumption, and minimum number of hops [29]. S.Diksha, Kamal give another protocol with finest data communication route with heterogeneous sensor nodes in LEACH [30]. D. Deepak , et. al. introduced energy efficient distributed algorithm. They compare the LEACH protocol with EE-LEACH protocol on simulator and found in results that EE-LEACH reduced the consumption of energy approximate 43% as compare to LEACH [31]. A hybrid clustered scheme K-Means and LEACH algorithm based, is presented by M.Aziz, et. al. for energy optimization [32]. Chunyao FU,et. al. presented new algorithm to intended balanced the entire networks consumption and enhance network lifespan [33].

Watermarking LEACH protocol [5] does work with proposition of data integrity and novel energy efficient of WSN. Cryptography is best security algorithm which maintains the integrity of sensed data. To confirm data authenticity and data integrity in sensor network digital watermarking technique might be use. Watermarking LEACH provide integrity using cryptography technique with LEACH protocol. But limitation of watermarking LEACH is it provide integrity only at cluster head level not at node level.

IV. PROPOSED REVINED R- WATERMARKING LEACH PROTOCOL

Our proposed R-Watermarking Leach algorithm is extended edition of watermarking LEACH algorithm. To improve the integrity and privacy of sensor network is the main principle of R-Watermarking LEACH. Watermarking LEACH protocol has integrity only at cluster head level and privacy has not considered in this protocol. But our proposed R-Watermarking LEACH routing protocol, have integrity at both node level as well as Cluster Head level by using watermarking technique. And our proposed algorithm maintains the privacy by the use of encryption schemes.

Our proposed R-Watermarking Leach protocol has two states:

- Setup state
- Steady state

The working of R-watermarking LEACH is done in several rounds here every round have two states. At time of process each round start with cluster formation in set-up state and ends with steady state.

A. Set-up phase

The set-up state, make the clusters and select the CH a node have maximum energy for each formed cluster from all the sensor nodes.

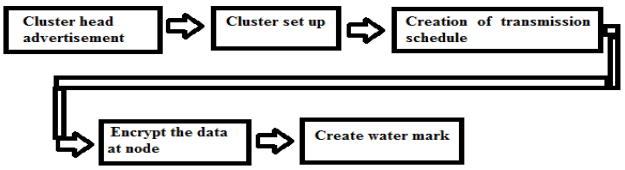

Fig. 1. Fundamental steps of set-up phase

In setup state, first CHs are randomly selected. When a sensor node is elected for CH, it release an adv-msg. Adv-msg contain the information qualify for the CH. CH hear advertisement with highest signal force is belonging CH. Then it give information to CH that it's a node of this cluster with sending a reverse message to CH.

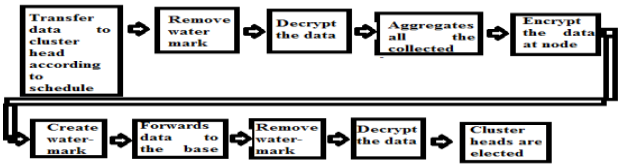

Fig. 2. Steps of Steady phase

TDMA schedule generated by the CB is based on total no. of nodes present in cluster. TDMA schedule decide the time of data transmission.

B. Steady state

In second state, cluster members sensed data from network area continuously add watermark on sensed data than decrypt the data and send it to particular CH in related clusters. When CH receives this data first it decrypts the data and remove watermark than aggregate all the collected data. Our proposed R-watermarking LEACH protocol provide double security node as well as CH level so, CH again add watermark to collected data and encrypt it then send data to the sink node.

V. PERFORMANCE EVALUATION

We simulate our proposed R-Watermarking LEACH routing protocol, using Matlab R2015a simulation tool, simulate with following parameters shown in Table 1 [2].

Table-I: Parameter value

Network Size	hundred × hundred m^2
No. of Sensor nodes	Hundred
Data aggregation energy	Five nJ/bit/signal
energy consumption for free space	Ten pJ/bit/m^2
Emp	Zero point zero zero one three pJ/bit/m^4
Message Size	Four Thousand bits

We simulate the performance with parameter Detection Rate. Figure 3 shows that hundred sensor nodes are randomly scattered in hundred by hundred m^2 network sizes and base station has placed at fifty by fifty m^2 here network length presented on axis-x and network height has presented on axis-y. These values are considered in meters. Here EDA means Data aggregation energy, is start with five nJ/bit/signal, Efs represent energy consumption for free space is ten pJ/bit/m^2 *and* we take message size is four thousand bits.

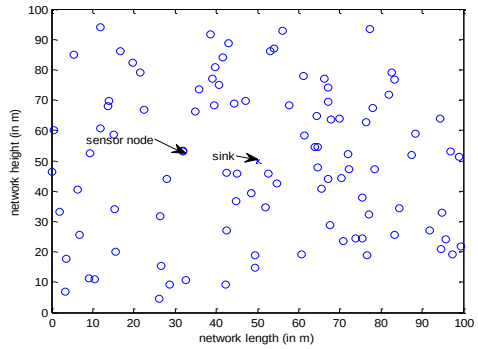

Fig.3. Performance evaluation with 100 × 100 m^2 Network Area

In figure 3 sensor nodes are represented with circle shape and base station is represented with ×.

Detection Rate

Detection Rate is the percentage of detection of falsification nodes by system. It is calculated by following formula:-

$$Detection\ Rate = \frac{N_1}{N_2} * 100 \qquad (3)$$

Where N_1 is number of falsification nodes detected by system and N_2 is total number of falsification nodes.

VI. SIMULATION RESULT

In our proposed R-Watermarking routing protocol all the falsification are detected at both level node and CH level, so detection rate is100% with R-Watermarking LEACH.

Table-II: Simulation result of R-Watermarking LEACH protocol with varying no. of round

Number of Rounds	R-Watermarking LEACH
100	100
200	100
300	100
400	100
500	100
600	100
700	100
800	100
900	100
1000	100

Simulation results for detection rate with deference to various no. of rounds for R- Watermarking LEACH routing protocol are shown in Table 2. Table 2 presents that Detection Rate is 100 percent with various number of rounds. It shows the detection rate is not affected by increased number of rounds.

In second phase we simulate it with increasing the number of falsification nodes:

Table-III: detection rate with respect to different no. of falsification sensor nodes for our proposed R-Watermarking LEACH

Number of Falsification Nodes	R-Watermarking LEACH
10	100
20	100
30	100
40	100
50	100
60	100
70	100
80	100
90	100
100	100

We simulate with number of falsification node increasing by 10. Table 3 shows that Detection Rate using R-Watermarking LEACH protocol is still 100 with various number of falsification sensor nodes. Table 3 show detection rate of proposed R-Watermarking LEACH routing protocol is same with different no. of falsification nodes.

VII. COMPARISON AND ANALYSIS

We compare Purposed R-Watermarking Leach protocol with Existing Watermarking LEACH protocol. We simulate both protocol in two ways- first with variant no. of rounds and second with various number of falsification node and found better result of R-Watermarking LEACH.

Simulation results for detection rate with various no. of round with R- Watermarking LEACH is compare with Watermarking LEACH are shown here Table 4.

Table-IV: Comparison table of Watermarking LEACH and R-Watermarking LEACH protocol with varying no. of round

Number of Rounds	PROTOCOL	
	Watermarking LEACH	R-Watermarking LEACH
100	37.4320	100
200	38.8829	100
300	33.5858	100
400	26.8639	100
500	22.4423	100
600	18.8720	100
700	16.8959	100
800	13.4735	100
900	13.3987	100
1000	12.0875	100

Table 4 illustrate Detection Rate occur in round 600 with R-Watermarking LEACH protocol is 100 and using Watermarking LEACH protocol is 18.8720. again Detection Rate occurs at round 900 using R-Watermarking LEACH protocol is 100 and using Watermarking LEACH protocol is 13.3987 and so on.

It shows in watermarking LEACH detection rate is decrease with increasing number of round but the R-Watermarking have same behavior for different no of rounds.

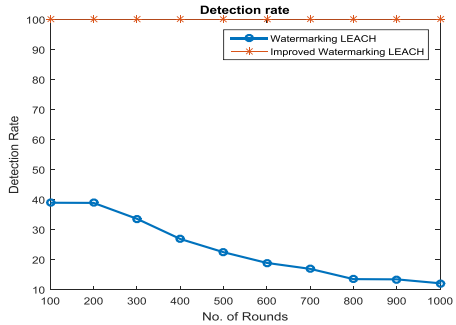

Fig. 4. shows the analytical graph of comparison of simulation values of detection rate with varying number of round of R-Watermarking LEACH and Watermarking LEACH.

As per Figure 4 if the number of rounds are increased in watermarking then detection rate is comparatively decrease but in R-watermarking LEACH is still same with varying number of round. Figure 2 shows that Detection Rate of R-Watermarking LEACH is better than Watermarking LEACH protocols.

In second phase we simulate it with increasing the number of falsification nodes:

Table-V: detection rate with various no. of falsification nodes with R-Watermarking LEACH and Watermarking LEACH

Number of Falsification Nodes	PROTOCOL	
	Watermarking LEACH	R-Watermarking LEACH
10	37.8641	100
20	32.1002	100
30	30.4514	100
40	26.8850	100
50	24.4604	100
60	22.5513	100
70	21.1386	100
80	19.7007	100
90	18.7378	100
100	17.5668	100

We simulate with number of falsification node increasing by 10. Table 5 shows that Detection Rate using R-Watermarking LEACH protocol is 100 and using Watermarking LEACH protocol is 30.4514 using 30 no. of falsification nodes. With 90 falsification nodes detection rate of watermarking leach is 18.7378 and in R-Watermarking is still same.

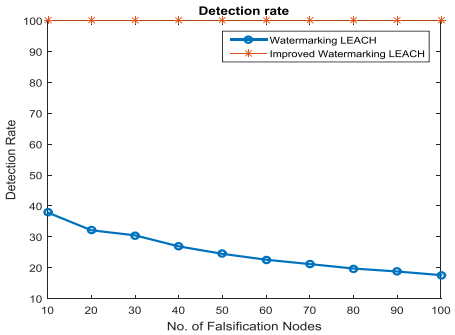

Fig. 5. Shows the analytical graph of comparison of simulation values of detection rate of R-Watermarking LEACH and Watermarking LEACH.

Table 5 show when the falsification nodes are increased detection rate of Watermarking LEACH is decrease but R-Watermarking is same with various no. of falsification nodes.

Figure 5 presents if no. of falsification nodes are increased with Watermarking LEACH then detection rate is comparatively decreased but in our R-watermarking LEACH are still constant. Simulation result shows that Detection Rate of R-Watermarking LEACH is improved than Watermarking LEACH protocols with varying no of falsification nodes

VIII. CONCLUSION

This paper, analyses the performance of R-Watermarking LEACH and Watermarking LEACH based on detection rate. Which are compared with two parameter varying number of round and number of falsification nodes.

We present with simulation results that our proposed R-Watermarking LEACH algorithm give better detection rate in comparison of Watermarking LEACH algorithm. In future, we will introduce an energy efficient protocol and analysis the performance.

REFERENCES

1. G. Pottie and W. Kaiser, "Wireless integrated network sensors," Communications of the ACM, vol. 43, no. 5, pp. 51–58, May 2000.
2. B., I., S., D. Morgera and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," Communications Surveys & Tutorials, IEEE 16, no. 1 (2014), pp. 266-282.
3. M. Messai, "Classification of Attacks in Wireless Sensor Networks", International Congress on Telecommunication and Application, April 2014, pp.23-24.
4. S. and J., "A Survey on Wireless Sensor Network Security," International Journal of Communication Networks and Information Security (IJCNIS) 1, no. 2 (2009).
5. Nejla Rouissia, Hamza Gharsellaouib, "Improved Hybrid LEACH Based Approach for Preserving Secured Integrity in Wireless Sensor Networks", International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES2017 ScienceDirect Procedia Computer Science 112 (2017) 1429–1438
6. E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks", book published by Wiley, 2009.
7. Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks", IEEE Commun. Surveys and Tutorials, vol. 8, num. 2, pp. 2–23, 2006.
8. C. Yadav, K. Raksha, S. Supriy, A. Hegde, N.C. Anjana and S. Kumar , "E, Security Techniques in Wireless Sensor Networks : A Survey", International Journal of Advanced Research in Computer and Communication Engineering, vol. 4, Issue 4, April 2015.
9. A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler, "SPINS: Security protocols for sensor networks", Wireless networks, pp. 8,521-534, 2002.
10. H. Cam, "Nonblocking OVSF Codes and Enhancing Network Capacity for 3G Wireless and Beyond Systems", To appear in the Special Issue of Computer Communications on "3G Wireless and Beyond For Computer Communications", Spring 2003.
11. Cam, H., S. Ozdemir, Muthuavinashiappan, D., & Nair, P., "Energy efficient security protocol for wireless sensor networks", IEEE 58th Vehicular Technology Conference, 2003, pp-2981-2984
12. Karlof, C., & Wagner, D., "Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, 2003, vol. 1, pp. 293–315.
13. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. Tygar, SPINS: "security protocols for sensor networks", In: Proceedings of Mobile Networking and Computing , 2001.
14. Çam, H., Özdemir, S., Nair, P., Muthuavinashiappan, D., & Ozgur Sanli, H. (2006). Energy-efficient secure pattern based data aggregation for wireless sensor networks. Computer Communications, vol. 29, no.4, pp. 446–455.
15. Nasser, N., & Chen, Y., "SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks", Computer Communications,2007,vol.30,pp.2401–2412. doi:10.1016/j.comcom.2007.04.014
16. Mukherjee, N., "A Dynamic Cryptographic Algorithm to Provide Nodal Level Security in Wireless Sensor Network", International Conference on Innovative Computing and Communication , 2010.
17. Rekha Rani, Rajan Manro, "Improved Watermarking Leach Protocol using node level Integrity and Confidentiality in WSN, international journal of computer science and engineering, Vol-6, Issue-11 Nov-2018 E-ISSN 2347-2693.
18. J. Zhou, "Efficient and Secure Routing Protocol Based on Encryption and Authentication for Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2013.
19. W.R. Heinzelman, A. P. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks",Proc. of the 33rd IEEE Int. Conf. on System Sciences,Honolulu, USA, Jan. 2000, pp. 1–10.
20. X. H. Wu, S. Wang, "Performance comparison of LEACH and LEACHC protocols by NS2," Proceedings of 9th International Symposium on Distributed Computing and Applications to Business, Engineering and Science. Hong Kong, China, pp. 254-258, 2010.
21. Z. PENG, L. Xiaojuan, "The Improvement and Simulation of LEACH Protocol for WSNs", IEEE pp-500-503.
22. Arumugam, G. S., & Ponnuchamy, T., " EE-LEACH: development of energy-efficient LEACH Protocol for data gathering in WIRELESS SENSOR NETWORK",. EURASIP Journal on Wireless Communications and Networking, 2015.
23. D. Mahmood1, N. Javaid1, S. Mahmood2, S. Qureshi3, A. M. Memon4, T. Zaman , " MODLEACH: A Variant of LEACH for WSNs" 2013.
24. Manjeshwar, A., & Agrawal, D. P., "APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless". Proceedings 16th International Parallel and Distributed Processing, 2002.
25. A. and H. Kong, "Energy Efficient Cooperative LEACH Protocol for Wireless Sensor Networks", JOURNAL OF COMMUNICATIONS AND NETWORKS, vol. 12, no. 4, August 2010, pp. 358-365.
26. L. Lanyingi, L. Changdong, "An Improved Algorithm of LEACH Routing Protocol in Wireless Sensor Networks", 8th International Conference on Future Generation Communication and Networking, 2014.
27. Mbarek, B., & Meddeb, A., "Energy efficient security protocols for wireless sensor networks : SPINS vs TinySec", International Symposium on Networks, Computers and Communications (ISNCC), 2016.
28. N. Mittal,, D. Singh, A. Panghal, R.S. Chauhan, "IMPROVED LEACH COMMUNICATION PROTOCOL FOR WSN NCCI", National Conference on Computational Instrumentation CSIO Chandigarh, INDIA, 2010, pp. 153-157
29. E. Christina, D. P. S., & J. Chitra, R., " Energy efficient secure routing in wireless sensor networks", International Conference on Emerging Trends in Electrical and Computer Technology, 2011.
30. D. Sharma, K., "Survey of energy efficient leach protocol in WSN", International Journal of Engineering Development and Research, vol. 4, Issue 3, 2014.
31. Dr. D. Dembla, H. Shivam, "Energy Efficient LEACH protocol for Wireless Sensor Network (EE-LEACH)", IJITKMI, vol. 6, no. 2, December 2013, pp. 165-169.
32. A. Mahboub1, M. Arioua2, E. En-Naimi3, " Energy-Efficient Hybrid K-Means Algorithm for Clustered Wireless Sensor Networks", International Journal of Electrical and Computer Engineering (IJECE), vol. 7, no. 4, August 2017, pp. 2054-2060.
33. C. FU1, Z. JIANG1,W. WEI2 and A. WEI, "An Energy Balanced Algorithm of LEACH Protocol in WSN", IJCSI International Journal of Computer Science Issues, January 2013, vol. 10, Issue. 1, pp. 354-359.

AUTHORS PROFIE

Ms. Rekha, rani had done Master of computer application from *Kurukshetra University* in 2004 and M.phil from choudhary Devi Lal university in 2008. She is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Sciences, Guru Nanak College, Budhlada since 2005. she is a member of computer society of India since 2010. she has published more than 14 research papers in national and international reputed journals and IEEE,CSI,UGC etc. approved conferences and published three books. She is having minnor project from UGC. Her main research work focuses on wireless sensor network, Network Security, Cloud Security and Privacy. She has 12 years of teaching experience and 4 years of Research Experience.

Dr. Harmaninderjit singh, is an Associate Professor and has more than 12 years of academic experience. He has done MCA degree from Punjabi University Patiala, Punjab, India and received the P.hd Degree in Computer Science from Desh bhagat university, Mandi gobindgarh, India. He had published more than 17 papers in different Journals and conference proceedings. His research interest is in the areas of Open Source Software and Algorithm Design and is presently working on it.