IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

Improved Watermarking Leach Protocol using node level Integrity and Confidentiality in WSN

Rekha Rani[1*], Rajan Manro[2]

[1]Department of Computer Science(Desh Bhagat University),Mandi Gobindgarh,India
[2]Department of Computer Science(Desh Bhagat University),Mandi Gobindgarh, India

Available online at: www.ijcseonline.org

Accepted: 26/Nov/2018, Published: 30/Nov/2018

Abstract— Wireless sensor network is a network which consists of number of sensor nodes which sense the data and send to sink node. As detecting sensor data with defective readings is an important issue for secure communication. So, necessity of privacy and integrity of information is mandatory. Thus, cryptography is an effective technique that provides privacy and integrity to sensed data. This paper, deals with the improvement of watermarking LEACH with node level data integrity and confidentiality.

Keywords— *WSN*, integrity, confidentiality, watermarking

I. INTRODUCTION

Wireless sensor networks can be described as an emerging technology with a very promising future [1]. Wireless sensor systems (WSNs) can be setup in a broad area to look at physical incident with acceptable accuracy and reliability [33]. The sensors can sense a variety of objects, for example, humidity, motion, pressure and temperature. Sensor nodes may impulsively form network, dynamically familiarize to device let-down and scarcity, control the movement of sensor nodes, and react to variations in job and network necessities[2][3]. Each individual sensor contains both working and communication of objects and is planned to sense the surroundings for event occur by the objects. [4]. Routing techniques and security issues are big research challenge with WSN. By time has been number of routing protocols have been devised for this [5], which can be sorted into two classes: flat routing protocol and hierarchical routing. These days in WSN, numerous hierarchical protocols have been proposed for WSN however most popular protocol is LEACH. Hierarchical routing protocols are defined to reduce energy consumption by aggregating data and to reduce the transmissions to the base station [6]

An outline of this paper is as follows. Section II presents WSN Architecture. Section III presents the wireless sensor network applications. Section IV presents types of routing protocols. Section V presents Improved Watermarking Leach. Section VI presents conclusion and future scope.

II. WSN ARCHITECTURE

It consist of microcontroller unit antenna, receiver and transmitter sensor and control units are connected to the battery for required power supply voltage sensor sense the physical environment and send the input to the A/D converter to convert it into digital form and then it is send to the control unit of microcontroller from where the outputs are controlled by the mechanism stored in microcontroller unit [32].

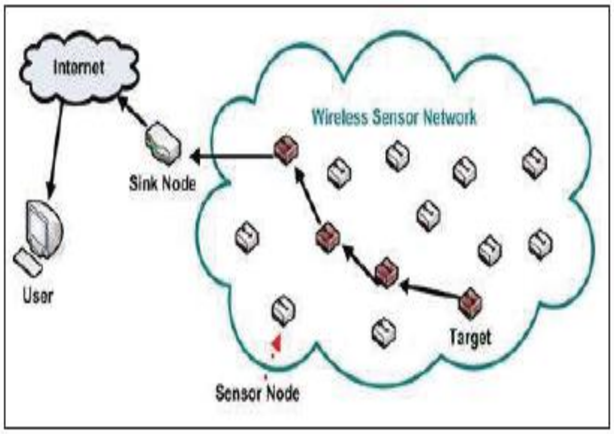

Fig.1. WSN Network

III. WIRELESS SENSOR NETWORK APPLICATIONS

Wireless sensor networks may comprise of numerous different types of sensors like low sampling rate, seismic, magnetic, thermal, visual, infrared, radar, and acoustic, which are clever to monitor a wide range of ambient situations. Sensor nodes are used for constant sensing, event ID, event detection & local control of actuators. The applications of wireless sensor network mainly includes

Military Applications[7],Health Applications, Health care monitoring, [8],Environmental Applications, Home Applications, Commercial Applications, Area monitoring, Environmental/Earth sensing's, Air pollution monitoring[9], Forest fire detection, Landslide detection, Water quality monitoring, agriculture and food Industrial monitoring[10].

IV. TYPES OF ROUTING PROTOCOL

Flat Routing Protocol: In flat routing protocol each node in the sensor network typically play the same role and all sensor nodes combines together to perform the sensing task[11][25][26].

Location Based Routing Protocol: In Location based routing protocols acknowledge by distance between the neighbouring nodes and distribution of the sensor nodes in the network area. These protocols are based on two assumptions 1) It is assumed that every node in the network have the knowledge of the neighbouring node position in the network. 2) The message is the source of information about the destination node position [29][30]. The hello messages are periodically transmit by the nodes for gathering the information about the neighbour node position. Therefore, once the destination node location is known all the operations are performed locally [24][31].

Hierarchical Routing Protocols: Hierarchical routing protocols are different from flat routing protocols, the nodes are not similar and they play different role. In hierarchical protocol nodes which have higher energy level can be used for processing data and for sending the information whereas the nodes which have lower energy level used for sensing [12,13]. In this type of protocols nodes are organized in clusters. The cluster has the cluster head which are elected by using different cluster head election techniques. The cluster head are used for the special task i.e. for high level communication. In this paper, We will discuss various hierarchical routing protocols [27][28].

LEACH (Low Energy Adaptive Cluster Hierarchy) **protocol**
LEACH protocol (based on hierarchical clustering algorithm) was presented by W.R.Heinzelman, [14] for wireless sensor networks. In LEACH the intention is alienated into rounds, in each round an alternate group of nodes are cluster heads (CH). For the time of processing all the nodes are divided into few groups called cluster. In each group a head node is selected to organize the cluster is called cluster head other nodes are called cluster-member. Each round can be separated into two stages: set up phase and steady state phase. The time and vitality expended in the last stage is longer than that in the previous.

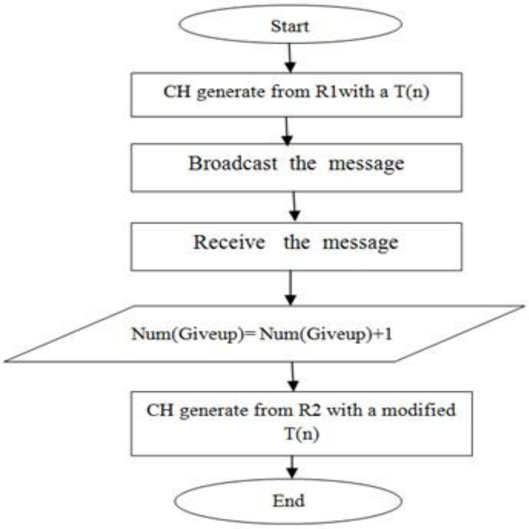
Start
CH generate from R1with a T(n)
Broadcast the message
Receive the message
Num(Giveup)= Num(Giveup)+1
CH generate from R2 with a modified T(n)
End

Fig. 2. Flow chart of leach algorithm[6].

A. Set-Up Stage

In the set-up stage [15], a random number the sensor nodes produce a number between 0 and 1 arbitrarily. Compared with T(n), the node will be chosen as cluster head if the produced number is less than the threshold. The cluster head node communicates data to nearby nodes, and the others pick the cluster to join according to the intension of the broadcast data. At that point, the cluster head utilize the approach of TDMA to disperse the time period of data transmission for members.

$$T(n) = \begin{cases} \dfrac{P}{1 - P * (r \bmod \dfrac{1}{P})} & if\ n \in G \\ 0 & if\ n \notin G \end{cases}$$

In the second phase [16], the collected data packets are delivered from cluster member to cluster head, at last data sent to sink node by cluster-head. The sink node exchanges the gathered data to the monitor centre for further processing. The cluster-heads should process data fusion and communicate with sink node, which costs much energy of the cluster-heads. Thus, after certain time, the network ought to be revised, and this methodology would be continuously circulated. [17]

B. Water Marking Leach

Energy-efficiency and data integrity is mandatory for requirement of information. Cryptography is an effective technique for maintaining integrity to sensed data. With sensor restriction, we cannot exchange traditional cryptographic algorithm to WSN. Watermarking LEACH is also a version of LEACH hierarchical routing protocol on watermarking for WSN, which is working with the proposition of a novel energy efficient and data integrity of wireless sensor network. Digital watermarking might be utilized to confirm data integrity or authenticity in WSNs.

The main advantage of this algorithm to secure the digital rights and embed the relevant data. Along these lines, watermarking data is straightforwardly connected with sensor information. Redundant space of the information is utilized to store the advanced watermarking information. Watermarking data is generated and embed at source sensor nodes but its verification is done at sink level [19][20][21].

Due to inherent organization nature and energy restraint constraint of sensors in wireless sensor networks, ensuring energy efficiency together with the security of the sensor data winds up primordial. This approach treats at the same time energy efficiency by utilizing the Watermarking LEACH a cluster-based data routing algorithm and secure data communication against falsification to ensure data integrity based on watermarking to LEACH delivering a modified data to a base station. So, Watermarking LEACH overcomes this disadvantage by checking integrity by using watermarking technique. This protocol mainly focuses on data integrity because it is one of major concerns in security of IOT[18]. At the steady phase, CH has all data collected from sensors in its cluster based on Time Division Multiple Access (TDMA). So, CH generates the watermarking information (mark1) according to figure 3 then, aggregates and transmits it to the base station (BS). At the BS, when receiving all data, extract the watermarking information. Thus the watermarking information is expressed a (mark2).

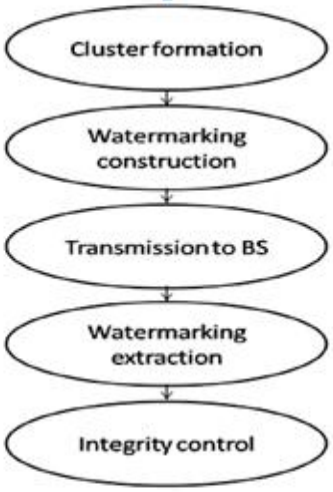

Fig.3. Flow Chart of our proposed Water-marking Leach

In extraction step, BS recalculates the watermark, if mark1 is equal to mark2 the data integrity has not been falsificated during the transmission [22][23].

V. Improved Watermarking LEACH

Our purposed algorithm is improved version of watermarking LEACH protocol. Watermarking LEACH only works with the proposition of a novel energy efficient and data integrity of wireless sensor network. It works are construct just on cryptographic technique which accomplishes data integrity but this protocol has not been considered privacy. In Watermarking LEACH data is generated and embed at Cluster Head level not at node level and directly its verification is done at Base Station level. In watermarking LEACH there was no integrity at node level and privacy has not been considered. But in our proposed algorithm we will provide integrity at node level as well as Cluster Head level by using watermarking technique and maintain privacy by using encryption techniques.

In this approach data has not been transfer directly destination to source, before transmitting the data from node to CH each node generate a watermark named mark1 that is used by cluster head for checking integrity of node data as well as each node encrypt the data so, node send the encrypted data with mark1 to CH. After that CH decrypt the data and generate a new watermark named mark2. Here CH compare the data if mark1 match with mark2 then it verify that there was no modification in data otherwise discard the data.

After collecting the data from all associated nodes CH aggregate the data. Aggregated data is encrypted before sending the data to the sink node and again generate watermark named mark3. Sink node first decrypt the data and generate watermark named mark4. And again check If mark3 match with mark4 then it verify that there was no modification in data otherwise discard the data.

In the set-up stage, after sensing the data first node encrypts this data and generate watermark (mark1). The cluster head node communicates data to nearby nodes, and the others pick the cluster to join according to the intension of the broadcast data.

At the steady phase, the cluster head decrypt the received data and aggregate all the received data from various cluster members. Then before transmitting create a new watermark (mark3). And compare both watermark if mark1 is same as mark2 there is no modification in data otherwise discard the data.

CH generates the watermarking information (mark1) then, aggregates and transmits it to the base station (BS). At the BS, when receiving all data, extract the watermarking information. Thus the watermarking information is expressed as (mark2). In extraction step, BS recalculates the watermark, if mark1 is equal to mark2 the data integrity has not been falsificated during the transmission.

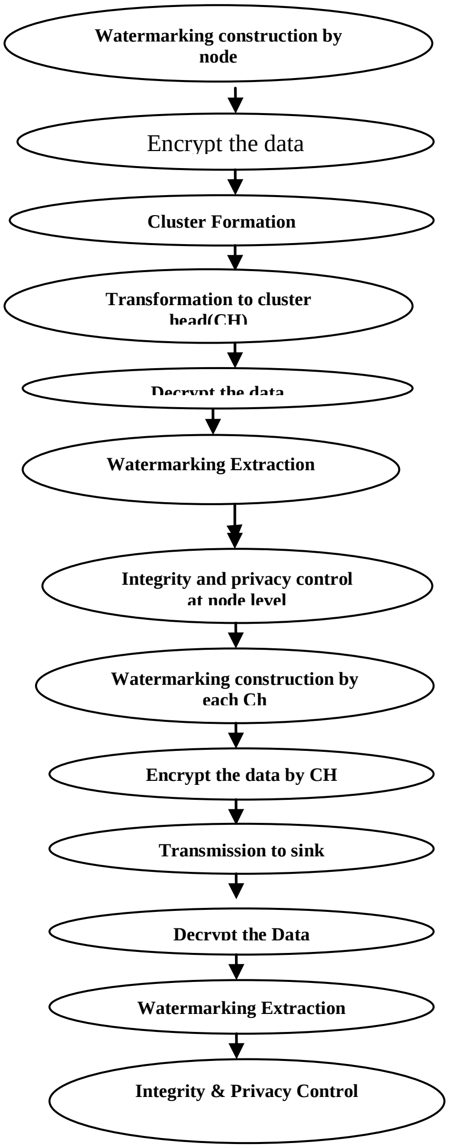
Watermarking construction by node
Encrypt the data
Cluster Formation
Transformation to cluster head(CH)
Decrypt the data
Watermarking Extraction
Integrity and privacy control at node level
Watermarking construction by each Ch
Encrypt the data by CH
Transmission to sink
Decrypt the Data
Watermarking Extraction
Integrity & Privacy Control

Fig.4. Flowchart of Improved watermarking LEACH

Table1. Comparison of Improved watermarking LEACH Protocol with Watermarking LEACH and LEACH Protocol

	LEACH	**Watermarking-LEACH**	**Improved Watermarking-LEACH**
Integrity at node level	No	No	Yes
Integrity at CH level	No	Yes	Yes
Privacy at node level	No	No	Yes
Privacy at CH level	No	No	Yes

VI. Conclusion and Future Scope

This paper work presents the first privacy and integrity of data that attempts to add security based on watermarking and cryptographic technique to watermarking LEACH called improved watermarking-LEACH with the aim of achieving data integrity and privacy. The main contribution of our work is to treat privacy and integrity at both level node and CH level. It has been concluded that our proposed protocol is better then Watermarking-LEACH at level of security. In future we will simulate this protocol on different simulator and compare the performance of existing Watermarking with our proposed improved Watermarking-LEACH

References

[1] S. chowiak, P., "Cryptographic Key Distribution In Wireless Sensor Networks Using Bilinear Pairings," PhD diss., Dublin City University, 2010.

[2] S., A. Reisslein, M.Towards, "Efficient wireless video sensor network: A survey of existing node architecture and proposal for a flexi-WVSNP design", IEEE commun.surv. Tutor, pp. 462-486, 2011.

[3] B. Tavli, K. Bicakci, R. Zilan and B. Ordinas, J.M., "A survey of visual sensor network platforms multitimed Tools", pp. 689-726, 2012 .

[4] N. kumar, J. Kaur "Improved LEACH Protocol for Wireless Sensor Networks", IEEE 2011.

[5] Reshma I. Tandel , "Leach Protocol in Wireless Sensor Network: A Survey", International Journal of Computer Science and Information Technologies, pp. 1894-1896, 2016.

[6] B. Zhenshan, X. Bo and Z. Wenbo. "HT-LEACH: An Improved Energy Efficient Algorithm Based on LEACH", International Conference on Mechatronic Sciences, Electric Engineering and Computer (MEC), 2013.

[7] M. Pejanović Đurišić , Z. Tafa and G. Dimić , "A survey of military applications of wireless sensor networks" Mediterranean Conference on Embedded Computing (MECO), IEEE 2012.

[8] K. JeongGil, L. Chenyang, B. Mani,. Srivastava , A. John, Stankovic and Andreas , " Wireless Sensor Networks for Healthcare", Proceedings of the IEEE, pp. 1947 – 1960, Nov. 2010.

[9] Y. Dunfan, D. Gong and W. Wang, "Application of wireless sensor networks in environmental monitoring", 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), IEEE 2009.

[10] L. Ruiz-Garcia ,L. Lunadei, P. Barreiro and I. Robla, "A Review of Wireless Sensor Technologies and Applications in Agriculture and Food Industry: State of the Art and Current Trends" , pp.4728-4750,2009.

[11] Nikolas, A. Pantazis, Stefanos, A. Nikolidakis and Dimitrios D. Vergados, "Energy – Efficient Routing Protocols in Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials.

[12] A. Gupta and A. Nayyar, "A Comprehensive Review of Cluster-Based Energy Efficient Routing Protocols in Wireless Sensor Networks", International Journal of Research in Computer and Communication Technology, 2014.

[13] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks,pp. 393–422, 2002.

[14] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor

networks," in 33rd Annual Hawaii International Conference on System Sciences, pp. 3005 – 3014,2000.

[15]R. Patel, S. Pariyani and V. Ukani," Energy and hroughput Analysis of Hierarchical Routing Protocol(LEACH) for Wireless Sensor Networks", International Journal of Computer Applications, 2011.

[16] Y. Ren Tsai, "Coverage Preserving Routing Protocols for Randomly Distributed Wireless Sensor Networks", IEEE Transactions on Wireless Communications, 2007.

[17] J. FENG YAN, " Improved LEACH Routing Protocol For Large Scale Wireless Sensor Networks", YUAN-LIU LIU School of Computer Science & Technology Soochow university Soochow 215006, China, IEEE 2011.

[18] Nejla Rouissia and 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, pp. 1429-1438, 2017.

[19] B. Djallel Eddine, S. Boubiche and A. Bilami, "A Cross-Layer Watermarking-Based Mechanism for Data Aggregation Integrity in Heterogeneous WSNs" Communications Letters, IEEE, 2015.

[20] G. Kaur, N. Kumar, "Secure and Efficient Data Collection in WSN", International Journal of Advanced Research in Computer Science and Software Engineering, 2015.

[21] DG. Costa ,S. Figuerłdo and G. Oliveira, "Cryptography in Wireless Multimedia Sensor Networks: A Survey and Research Directions", 2017.

[22].A.Singh, M.Marwaha, B.Singh, S.Singh, "Comparative Study of DES, 3DES, AES and RSA", International Journal of Computers and Technology, 2013.

[23]P.Pritto Paul, N.Sankar Ram and M.Usha, "Symmetric Key Encryption for Secure Communication Using Wireless Hart in Wireless Sensor Networks (WSN)", Australian Journal of Basic and Applied Sciences, 2016.

[24] Zhang, J., R. Shankaran, M.A. Orgun, V. Varadharajan, A. Sattar, "A trust management architecture for hierarchical wireless sensor networks. In Local Computer Networks (LCN)", IEEE 35th Conference ,pp: 264-267,2010.

[25] H. P. Keeler, P. G. Taylor, "A stochastic analysis of a greedy routing scheme in sensor networks", SIAM Journal on Applied Mathematics, pp. 2214-2238, 2010.

[26] W. R. Heinzelman, J. Kulik, H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", in Proceedings of the 5th annual ACM/IEEE international conference on Mobile computing and networking, Seattle, Washington, USA, pp. 174-185, 1999.

[27] X. Liu, "A Survey on Clustering Routing Protocols in Wireless Sensor Networks", Sensors, pp. 11113-11153, 2012.

[28`] S. Naeimi, H. Ghafghazi, C.-O. Chow, H. Ishii, "A Survey on the Taxonomy of Cluster-Based Routing Protocols for Homogeneous Wireless Sensor Networks", Sensors, 2012.

[29] J. Grover, Shikha, M. Sharma, "Location based protocols in Wireless Sensor Network: A review", in Proceedings of the International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1-5,2014.

[30] Z. Kai, T. Libiao, L. Wenjun., "Location-Based Routing Algorithms for Wireless Sensor Network".Emerging Technologies of Future Multimedia Coding, Analysis and Transmission,2009.

[31] Y. B. Ko, N. H. Vaidya, "Location Aided Routing (LAR) in mobile ad hoc networks", Wireless networks, pp. 307-321, 2000.

[32] G. Sharma, A. Kumar, "REVIN: Reduced Energy Virtuous Immune Network for WSN", International Journal of Scientific Research in Computer Science and Engineering, Vol.5, Issue.2, pp.1-8, 2017.

[33] M. Bhardwaj, "Faulty Link Detection in Cluster based Energy Efficient Wireless Sensor Networks", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.3, pp.1-8, 2017

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 and editor in chief of international journol of information management and technology. she has published more than 10 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. Rajan Manro is an Associate Professor and has more than 14 years of academic experience. He has done MCA degree from GGNIMT, Ludhiana, Punjab, India, in 2004, the Post-Graduation Diploma in E-Commerce From ITI, Ludhiana, Punjab, India in 2001 and received the M.Phil Degree in Computer Science from Periyar University, Salem, India in 2008.He is certified Oracle -9i (DBA) Professional. He is an author of more than 30 books on different subjects like Java, ASP.Net, Artificial Intelligence, MIS, Expert System and RDBMS. More than 14 papers are published in different Journals and conference proceedings. His research interest is in the areas of Cloud Computing, E-Governance, A.I. etc. and is presently working on it.

.