International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Lightweight Security Protocol for Efficient Information Transfer in Sensor Networks

Andhe Dharani, Manjuprasad B

Abstract*: Wireless Sensor Networks have become major integral components of various other technologies like- IoT, Big Data, Cloud Computing and many. This impact is also making WSNs to grow more rapidly and its global market size is predicted to grow $944.92 million by 2020, at a CAGR of 12.96%. In-spite of this impact some challenges and application requirements in WSNs is there limiting its performance. In this article a detailed analysis and research has been carried out to address and resolve some of the major issues in the WSNs. This paper mainly aims in identifying and analyzing the major challenges and requirements along with some existing works in WSNs. Based on the identified problems this article presents the solution to increase the performance of WSNs. The main focus is given to energy and security aspects in the WSNs. The proposed protocol provides more strengthening security parameters with a focus on increasing the lifetime of the network in the resource constraint devices. The outcome of this paper is resulted in better results than the existing security and energy mechanism in the field of the wireless sensor networks.

***Keywords*: Wireless Sensor Networks, Sensors, Energy, Security, Clustering, LEACH, DBCH, SecLEACH, SLEACH**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) gaining huge impact in the recent years, and is set to rule the digital world with Internet of Things (IoT) in coming decade [1-2]. This impact of WSNs is due to the recent advancement in the sensors technology, wireless technology and real time applications. WSNs are now the major component of Internet of Things, Big Data, Cloud Computing and many other technologies. This application features are creating a huge impact in the growth of WSNs and its market size is predicted to rise from $401.23 Million in 2013 to $944.92 Million by 2020, at a compound annual growth rate (CAGR) of 12.96% from 2014 to 2020. The global markets of an application specific sensor devices are about to rise nearly from $2.4 billion in 2016 to nearly $7.7 billion by 2021 with a CAGR of 26.7% within these assessment years [3].

The global industrial WSNs market size is predicted to rise from $401.23 Million in 2013 to $944.92 Million by 2020, at a CAGR of 12.96% from 2014 to 2020. This report is also focused on the systems, sensors, technologies, applications, and geographies of the industrial sensor network. The global sensors market also creating its impact by an increase of its market value $101.9 billion to $113.2 billion from 2015 to 2016 and it is predicted to reach $190.6 billion by 2021, with a CAGR of 11.0% during 2016-2021. Among overall sensor ratings the image and chemical sensors are predicted to reach $51.2 billion by 2021, bio-sensor and fingerprint sensor are predicted to reach $44.5 billion by 2020 with a CAGR of 13.2% [4].

These statistics shows the impact of WSNs in the recent years in various sectors. This impact is due to the recent development in wireless communication and sensor technology. But majority of applications in WSNs comes with major challenges, problems and specific application requirements. These challenges are making WSNs an unstable and insecure in some of the domains.

This paper focuses on identifying some major problems in WSNs and proposes WSNs specific approaches to increase the performance of WSNs. This is achieved by streamlining the concepts in WSNs systematically into various sections. Section- 2 presents the WSNs application requirements and its challenges. Section-3 focuses on discussing and analyzing some of the existing works. Section-4 presents the proposed approaches for resolving the identified major problems. Section-5 compares the proposed approaches with some of existing standard benchmarks. Section-6 concludes the proposed work with its outcomes.

II. REQUIREMENTS AND CHALLENGES

This section focuses on the WSNs applications requirements and its challenges.

A. Requirements

- **Lifetime:** The lifespan of the WSNs depends on the individual sensor nodes which may affect the applications. The efficient utilization of the sensor energy is one of the major research challenges [5].
- **Availability:** Once the nodes are deployed for any kind of monitoring applications it must be available all the time. The data from the WSNs must not be lost. The need of WSNs is to collect the data from remote areas and it will be of no use if the data is not available when it is required.
- **Data Freshness:** The data collection from sensors should be very efficient in terms of throughput.

Manuscript published on 30 September 2019
* Correspondence Author
Dr. Andhe Dharani*, Department of MCA, R.V. College of Engineering, Bengaluru, INDIA, Email: andhedharani@rvce.edu.in
Dr. Manjuprasad B, Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, INDIA, Email: manjuprasad32@gsss.edu.in

The applications should not have any delay in transmitting the data to the central system. The delay in WSNs can affect the performance and functionality of the applications [6].

- **Security:** This is the major requirements in all the field and very crucial in WSNs military and surveillance applications. These applications should be trusted one, if the system is more vulnerable to threats and not able to resists the attack may lead to failure of whole applications [7].

B. Challenges

This section presents the various features of WSNs with its challenges:

- **Deployment:** Deploying the Sensor nodes are the initial task, this defines the network topology based on the number of nodes. This deployment may be random or fixed at specific location. And for small scale like building or campus monitoring may have nodes fixed at specific location and for large scale like forest or battle field it may have random deployment [8].
- **Lifetime:** The lifetime of the sensor network depends on the life span of the individual sensor nodes, which may depend on the amount of energy dissipated from the sensors for various operations. Lifetime of the WSNs is very crucial in all the application, the overall performance of the monitoring applications depends on this factor [9-11].
- **Security:** Wireless connections are more vulnerable to many types of attacks, WSNs also vulnerable to numerous threats related to information security [12-13]. Providing security in WSNs having constraints like- memory, battery, deployment area, low computational process make problem definition complex. This vulnerability have open door motivating factors like High communication overhead, high complexity, higher overhead whenever advanced cryptographic technique is used, which consumes more bandwidth.

III. ANALYSIS OF THE RELATED WORKS

This section discusses on the various existing resources utilization techniques and need of security with its challenges.

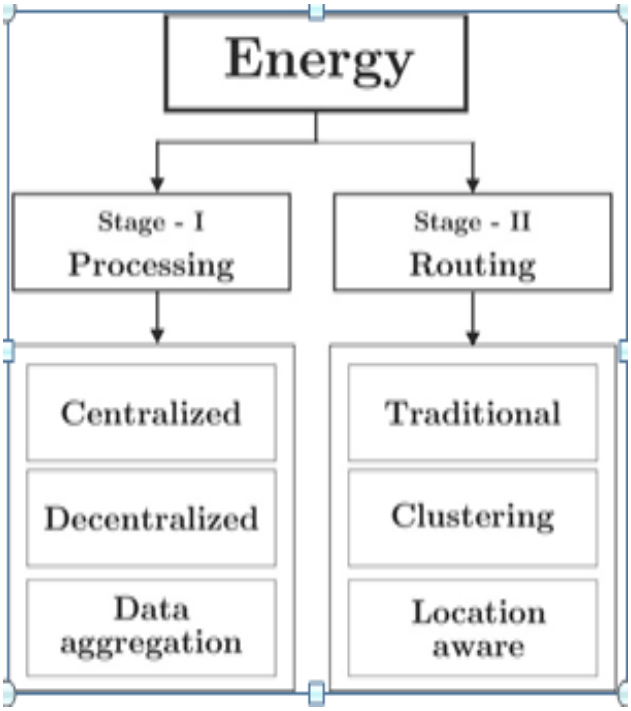

Fig. 1. Energy consumption Classification

The background work carried here is classified into explicitly two categories – Category 1 - Energy & Performance as represented in fig-1; Category 2 - Security, for addressing the issues individually as represented in fig-2.

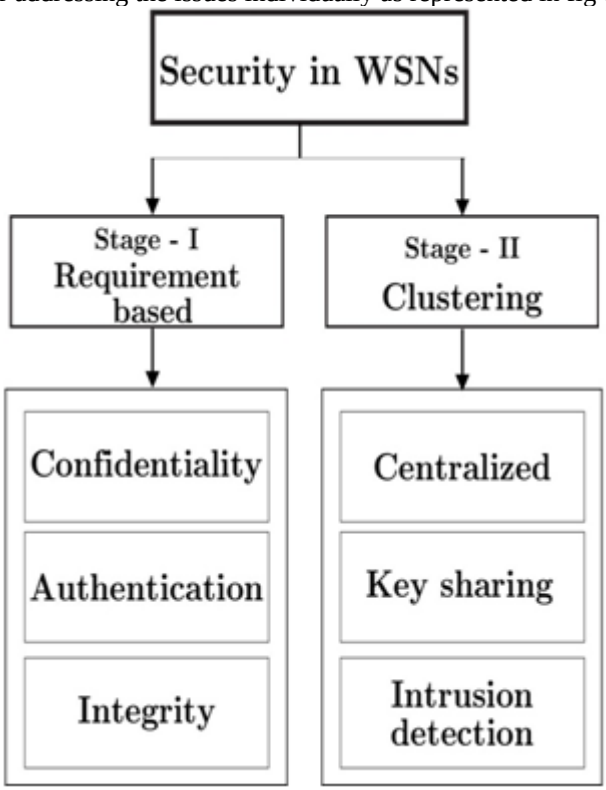

Fig. 2. Security Based Classification

Table-I. Analysis of Existing Energy based Protocols

Algorithm	Centralized / Decentralized	Data Aggregation	Hetero or Homogeneous	Analysis Carried out
Flossiping [14]	Centralized Routing Path	No	Homogeneous	Reducing duplicate packets
Gossiping [15]	Centralized Routing Path	No	Homogeneous	Reducing duplicate packets
HEED [16]	Decentralized Routing Path	Yes	Heterogeneous	Reducing overutilization of advance nodes
EECDA [17]	Decentralized Routing Path	Yes	Heterogeneous	Required a stable protocol to find the optimal number of cluster heads

Table - II. Analysis of Routing Protocols

Method	Lifetime Complexity	Computational Complexity	CH Selection	Analysis Carried out
Distributed Clustering				
LEACH [18]	Medium	Simple	Random	Integrating Uniform CH selection with a Residual Energy may increase the performance
Modified LEACH DT [19]	High	Simple	Probability based	Integrating Uniform CH selection with a Residual Energy may increase the performance
Centralized Clustering [20-21]				
Centralized & Decentralized Clustering Methods	Medium	Simple	By Base Station	Centralized Clustering may be efficient for data transmission but communication of initial processing with Base station may leads to more energy consumption
Centralized & Clustered K-coverage protocol	Medium	Simple	By Base Station	Initial processing with Base station may leads to more energy consumption
Residual Energy Based Clustering				
Energy & Node Concentration on Hierarchical Clustering	Medium	Simple	Residual Energy Based	No uniform CH selection which may require for avoiding redundant data

Table - III. Summary and Analysis of Security Protocols

Method	Working Mechanism	Security Achieved	Analysis Carried Out
A Secure key based Data Aggregation [22]	Based on the Elliptic Curve Cryptography	Integrity	Focused on Public key cryptography and Data aggregations
A Secure Location Aware Routing [23]	Key based secure mechanism with using a set of pair key for encryption	Confidentiality Authentication	Focused on Routing and security with a location aware mechanism
Counter Based Intrusion Detection [24]	Secure Key based routing protocol	Confidentiality Integrity Authentication	Focused on Secure Routing and Intrusion Detection
Trust aware secure routing [25]	Identity based secure routing protocol	Authentication	Focused on Security and Routing
An extended LEACH algorithm (LS-LEACH) with secure Routing Protocol [26]	A TDMA scheduled based routing protocol with a secure group key for cluster formation	Confidentiality	Each nodes maintained a 2 set of private key for secure data transmission
Secure Energy efficient Secure Directed Diffusion Protocol (ESDDP) [27]	A DDP based 3 set of key concept used for efficient securing of data with Individual Key, Pair-wise Key, Global Key	Confidentiality	Focused on reducing the energy consumption and thereby increasing the network lifetime

Based on the analysis of existing work [28-32], this paper further focuses on implementing the lightweight security approach with energy efficiency.

IV. PROPOSED SECURE CLUSTERING FOR EFFICIENT INFORMATION TRANSFER (SCEIT)

In this section an energy efficient secure clustering protocol is proposed. This proposed work concentrate on providing the security against eavesdropping, hello flood, Denial of Services(DoS), Packet Sniffing attacks in WSNs thereby maintaining the basic security requirements in WSNs. The working phases of this protocol are first phase is about the clustering model used for data transmission and second phase discusses on the working principles of the security part.

The model for this protocol is shown in the Fig. 3 which represents the numerous nodes deployed in an area of 100 sq.mt, where the Square node represent the base station for centralized processing activities, the 'x' and 'o' nodes represent the member nodes and the remaining shaded nodes are malicious nodes deployed for evaluating the efficiency of this protocol.

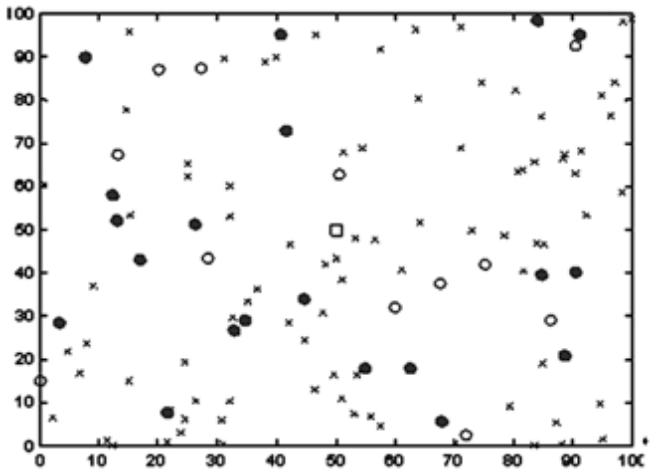

Fig-3. Network Representation

A Working of the proposed Security Protocol

Clustering Process

This is the first phase of our proposed method, where the actual Uniform Multihop CH distribution with Low Communication Overhead (UMLCO) will be done. This uniform CH distribution ensures efficient energy adopting 2 mathematical model discussed in this section. Threshold Distance for selecting cluster head is one model which is given by equation 1, which is derived based on the hexagonal cell structure as shown in Fig. 4. This hexagonal cell structure can avoid the overlap of the nodes within the nodes of other sensor nodes. This process also proposes threshold energy for selecting the cluster using sensing range which is as shown in equation 2. The working of this clustering process is described in the UMLCO clustering algorithm.

By using this threshold sensing range, uniform distribution of CH is ensured by selecting the nodes as a CH within the threshold sensing as given in the equation 3. This uniform distribution of CH reduces the communication overhead in the network and increase the lifetime of the sensor.

Fig-4. Hexagonal cell structure

$$Threshold-Sensing\left(T_s\right)=r+r \quad (1)$$

$$r=1/4\times R\sqrt{3} \quad (2)$$

where, r = Threshold sensing range; R = Actual sensing range

$$T_e=\left(\epsilon_u\times\epsilon_{da}\right)\times k+\epsilon_s\times k\left(T_d\times T_d\right) \quad (3)$$

where,

T_d : $\sqrt{\left(M_d^2+M_d^2\right)}$ = Threshold Distance

M_d : a/d = Minimum Distance

a : Network Area

d : Perimeter of the Network Area

ϵ_u: Transmitting Energy

ϵ_{da}: Data Aggregation Energy

k : Packet Size

Below is the Proposed Algorithm UMCLO

Algorithm 1 UMCLO

1 : *If Residual Energy* (R_e) > *Threshold Energy* (T_e) *then*
2 : *Calculate Threshold Sensing*
3 : *else*
4 : *Terminate CH request*
5 : *procedure CLUSTERING PROCESS*
6 : *If Distance between 2 CH* > *Threshold Sensing then*
7 : $CH \Rightarrow G$: id_{CH}, $Adv(id_{ch} \parallel position)$
8 : N_i : $Store(id_{CH}, min\left(Distance_{(BS-N_i)}, Distance_{(CH)}\right)$
9 : *if* $Distance_{(BS-N_i)}$ > $Distance_{(CH)}$ *then*
10 : $N_i \rightarrow CH$: $id_{Ni}\left(member_{request}, id_{CH}\right)$
11 : *else*
12 : $N_i \rightarrow BS$
13 : $CH \rightarrow N_i(id_{CH}, TimeSlot)$
14 : *else*
15 : *Terminate CH Request*

where

$\Rightarrow$: Broadcast

$\rightarrow$: Unicast

G : Set of Non CH nodes

N_i : Sensor nodes

id_{Ni} : ID of the sensor node

id_{CH} : ID of the CH

$Adv\left(id_{CH} \parallel position\right)$: Advertizing packet with ID of CH with its position as payload

BS : Base Station

CH : Cluster Head

$Distance_{(BS-Ni)}$: Distance from node to BS

$Distance_{(CH-Ni)}$: Distance from node to CH

B Securing Cluster

Using the UMCLO clustering process a novel secure clustering protocol is proposed. This Secure Information Transmission algorithm is described step by step with six main operations implemented as presented in Algorithm-Secure Information Transmission.

Retrieval Number: C5259098319/2019©BEIESP
DOI:10.35940/ijrte.C5259.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

The identification of DNS by BS and Nodes validation for becoming is also explained here in this algorithm. The third operation of this algorithm is sharing of a parity bit by the CH with the authenticated nodes identified by BS. The fourth stage of this algorithm is to ensure the originality of the packets received by CH from its member nodes with a set of rules and parity bit as depicted in algorithm. The fifth stage is transmission of the information to the BS with encryption technique which is explained in detail in next subsection of this chapter. The final operation of the algorithm is decryption of information at the BS which gives the original information sent by CH as in algorithm-2

Algorithm 2 Secure Information Transmission (SCEIT)

BS validates node information
procedure BS NOMINATES DNS
  $BS \Rightarrow G, Adv(n_i||n_{dns}||position)$
procedure DNS VALIDATES THE NODES BECOMING CH
  if Successful Validation **then**
    Nodes are Eligible for becoming CH
    $CH \rightarrow BS(id_{CH}$,Member info)
  else
    CH status reported to BS
procedure SECURING CLUSTER INFORMATION BY ASSIGNING A 1 BIT PARITY BIT
  $CH \rightarrow ni(id_{CH}, TimeSlot, ParityBit)$
procedure VERIFY PACKET RECEIVED AT CH BY FIREWALL RULES
  Rule-1: Verify Pre-registered ID or IP of nodes
  Rule-2: Verify Parity bit from registered nodes
  if Rule-1= True & Rule-2=True **then**
    Aggregate the Data at CH
  else
    Blacklist the nodes and status reported to DNS
procedure ENCRYPT THE INFORMATION AND TRANSMIT TO THE BS
  Set Key : $id_{CH} + id_{Round}$+ 1 bit Parity bit
  E(data)= $[Key] \oplus [data]$
  CH $\rightarrow$ BS(E(data))
procedure DECRYPT THE INFORMATION AT BS
  D(data)= $[Key] \oplus [E(data)]$

Where
$\Rightarrow$: Broadcast
$\rightarrow$: Unicast
G: Set of Non CH nodes
n_i : sensor nodes
id_{CH} : ID of the CH
Adv($id_{CH}||position$) : Advertizing packet with basic information as payload
Distance$_{(BS-ni)}$: Distance from node to BS
Distance$_{(CH-ni)}$: Distance from nodes to CH
n_{dns}: ID of DNS mapped to ni
Key : ID of CH know to Base Station
E() & D(): Encryption and Decryption function

SCEIT vs (SLEACH, SecLEACH, EEESDSN)

The contributed security protocol SCEIT is compared with the standard and recent clustering based secure protocols which are some of the existing protocols. SLEACH and SecLEACH are the LEACH based clustering secure protocols with integration of standard encryption techniques. EEEDSN which was published in year 2016 with an efficient approaches over SLEACH, SecLEACH secure clustering protocols. Table-IV shows the lifetime of the existing protocols with a basic simulation setup of 100 nodes, 2500 rounds, 0.5J Initial energy, 100mX100m Network area. Along with the SCEIT lifetime of the network.

Figure- 5 shows the security requirements achieved by the proposed secure clustering.

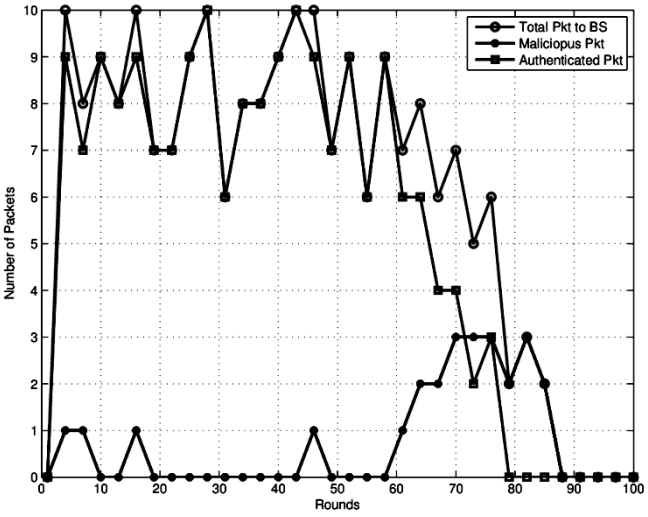

Figure-5: Total Malicious Packets blocked by the Proposed method

Table IV. Alive nodes percentage in the network

% of alive node	Sec LEACH	S-LEACH	EEE SDSN	SCEIT Proposed
100%	306	509	723	530
90%	450	592	885	730
80%	490	698	965	802
70%	542	780	1060	1025
60%	601	893	1110	1259
50%	764	1004	1202	1440
40%	814	1082	1370	1645
30%	901	1204	1530	1787
20%	976	1290	1707	2002
10%	1200	1354	1830	2143
0%	1300	1402	2103	2490

V. CONCLUSION

The proposed work here concludes with a secured system for efficient information transfer in sensor networks by implementing an security and energy integrated protocols. The implemented security protocol SCEIT resolves the issues associated with security in WSNs with its performance considerations.

These two protocols focused on providing energy efficient security approaches for WSNs by considering the resource constraints issues of the sensor nodes with security. These solutions proposed here are low communication and computational complexity which are specifically suitable of the sensor nodes. The proposed protocols were evaluated with the security strengthening parameters thereby defining its strength to resists major security attacks.

The results were compared with some of the existing protocols and with the self-evaluation in the presence of malicious nodes.

These security protocols found to be energy efficient by attaining the security requirements with low computational cost over identified performance metrics. Finally leading to a secured system for efficient information transfer in sensor networks. The simulation results achieved in this research article are specific and dependent of the hardware configurations of the sensors. The inclusion of high end hardware configurations with improved battery capacity, memory, storage and computing resources will increase the performance of the sensors.

REFERENCES

1. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, Vol. 38, 2002, pp. 393-422.
2. N. Bulusu, J. Heidemann, and D. Estrin, "GPS-Less low cost outdoor localization for very small devices," *IEEE Personal Communications Magazine*, Vol. 7, 2000, pp. 28-34.
3. T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for adhoc networks research," *Wireless Communications and Mobile Computing*, Vol. 2, 2002, pp. 483-502.
4. H. Chenji and R. Stoleru, "Toward accurate mobile sensor network localization in noisy environments," *IEEE Transactions on Mobile Computing*, Vol. 12, 2013, pp. 1094-1106.
5. Z. Guo, Y. Guo, F. Hong, X. Yang, Y. He, F. Yuan, and Y. Liu, "Perpendicular intersection: locating wireless sensors with mobile beacon," *IEEE Transactions on Vehicular Technology*, Vol. 59, 2010. pp. 3501-3509.
6. T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzher, "Range-free localization schemes for large scale sensor networks," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking*, 2003, pp. 81-95.
7. J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *Computer*, Vol. 34, 2001, pp. 57-66.
8. X. Li, "Collaborative localization with received-signal strength in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, Vol. 56, 2007, pp. 3807- 3817.
9. B. Liu, L. Cheng, H. Wu, Y. Chen, and F. Wang, "Ubiquitous localization method on mobile robot in the internet of things," in *Proceedings of International Conference on Modelling, Identification and Control*, 2012, pp. 537-542.
10. B. Mustapha, H. Abdelhakim, and B. Abderrahim, "High accuracy localization method using AOA in sensor networks," *Computer Networks*, Vol. 53, 2009, pp. 3076-3088.
11. D. Niculescu and B. Nath, "DV based positioning in adhoc networks," *Telecommunication Systems*, Vol. 22, 2003, pp. 267-280.
12. C. H. Ou and W. L. He, "Path planning algorithm for mobile anchor based localization in wireless sensor networks," *IEEE Sensors Journal*, Vol. 13, 2013, pp. 466- 475.
13. G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *ACM Communications*, Vol. 43, 2000, pp. 51-58.
14. N. B. Priyantha, A. Chakraborty, and H. Balakrishnan, "The cricket location-support system," in *Proceedings of the 6th ACM Annual International Conference on Mobile Computing and Networking*, 2000, pp. 32-43.
15. A. Savvides, C. C. Han, and M. B. Srivastava, "Dynamic fine-grained localization in ad hoc networks of sensors," in *Proceedings of the 7th ACM Annual International Conference on Mobile Computing and Networking*, 2001, pp. 166-179.
16. J. P. Sheu, P. C. Chen, and C. S. Hsu, "A distributed localization scheme for wireless sensor networks with improved grid-scan and vector-based refinement," *IEEE Tran- sactions on Mobile Computing*, Vol. 7, 2008, pp. 1110-1123.
17. M. L. Sichitiu and V. Ramadurai, "Localization of wireless sensor networks with a mobile beacon," *Center for Advances in Computing and Communications*, 2003, pp. 174-183.
18. K. F. Ssu, C. H. Ou, and H. Jiau, "Localization with mobile anchor points in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, Vol. 54, 2005, pp. 1187-1197.
19. M. Sugano, T. Kawazoe, Y. Ohta, and M. Murata, "Indoor localization system using RSSI measurement of wireless sensor network based on zigbee standard," in *Proceedings IASTED International Conference on Wireless Sensor Networks*, 2006, pp. 1-6.
20. G. Wang and K. Yang, "A new approach to sensor node localization using RSS meas- urements in wireless sensor networks," *IEEE Transactions on Wireless Communications*, Vol. 10, 2011, pp. 1389-1395.
21. Y. H. Wu and W. M. Chen, "Localization using a mobile beacon with directional antenna for wireless sensor networks," *IEICE Transactions on Information and Systems*, Vol. E94-D, 2011, pp. 2370-2377.
22. B. Xiao, H. Chen, and S. Zhou, "Distributed localization using a moving beacon in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, Vol. 19, 2008, pp. 587-600.
23. MAC IEEE RSSI-802.15.4, Standard for Information Technology-Part 15.4, "Wireless MAC and PHY specifications for LR-WPANS," 2006.
24. Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou," Sensor Network Security: A Survey". IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009.
25. D.W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and approaches for distributed sensor network security," NAI Labs Technical Report 00-010, 2000.
26. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," Commun. ACM, Special Issue: Wireless sensor networks, vol. 47, pp. 53–57, 2004.
27. Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain," An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks", International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012
28. Matthew N. Vella, Texas A&M Surveyof Wireless Sensor Network Security" *University-Corpus Christi, Computer Science Program, Dr. Ahmed Mahdy Texas A&MUniversity-Corpus* Christi, Computer Science.
29. Xiaojiang Du, North Dakota State University and Hsiao-HwaChen, National Cheng Kung University "Security in WirelessSensor Networks" IEEE Wireless Communication August 2008
30. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong"Security in Wireless Sensor Networks: Issues and Challenges" Feb. 20-22, *2006 ICACT 2006*
31. Benamar KADRI, Abdallah M'HAMED, Mohammed FEHAM. "Secured Clustering Algorithm for Mobile Ad hoc Networks", *International Journal of Computer Science and Network Security*, Vol.7, No.3, pp 27-34; March 2007.
32. Amanjot Kaur, "Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method", *International Journal of Scientific & Engineering Research*, Volume 4, Issue 5, May-2013 2212 ISSN 2229-5518

AUTHORS PROFILE

Dr. Andhe Dharani, Professor and Director, Dept. of MCA, RVCE, completed her Master of Computer Applications in 2000 from BMS College of engineering, Bengaluru. She pursued her Doctoral Research from Mother Theresa Womens University, Kodaikanal and obtained her Ph.D. in Jan 2010. She has undertaken and successfully completed funded research project "Power optimization in Adhoc sensor network" for the Naval Research Board, DRDO, New Delhi, 2011 – 2013, as Principal Investigator worth Rs. 10.95 Lakhs. She has guided more than 100 final year projects. She has so far published more than 70 papers in national and international journals and conferences. She has attended many international conferences, chaired many technical sessions and has reviewed papers for IEEE and other conferences. She received "Young Researcher Award" , By Cognizant - R.V. College of Engineering.

Dr. Manjuprasad B, Department of Computer Science and Engineering, GSSS Institute of Engineering and Technology for Women, Mysuru, INDIA, completed his B.E in CSE from VTU in 2011 and got an opportunity by Dr. Andhe Dharani to work as a her first Research Fellow for the project sponsored by DRDO under her supervision in 2011. During his research work he has gained >=24 credits for his Ph.D. Course Works, published 10 International Journal (05 Non Paid), 06 International Conference (3 Scopus Indexed) publications and presented 03 Open-Seminar at Research Centre. He received his Ph.D. from VTU, Belagavi in March 2019.