Cross-layer security solution for secure communication of sensorsin Wireless Sensor Networks

Rakesh Kumar Saini[1] , Naveen Kumar[2]
[1]Department of Computer Science and Application, DIT University, Dehradun
Uttrakhand, India
[2]Department of Computer Science & Engineering, DITUniversity, Dehradun
Uttrakhand, India
rakeshcool2008@gmail.com[1]
naveen.it23@gmail.com[2]

ABSTRACT

Safe path-finding is extremely necessary for multi hop wireless systems such as Wireless Sensor Networks. Multihop wireless systems are more unprotected to safetyoutbreaks as associated to single-stage wireless networks.Cross-layerdesign production is a precise significant character for wireless sensor network submissions. Advancedsecurity is significant for the achievement of announcement among sensor nodes in wireless sensor network because the numbers composed is regularly less and the network is most vulnerable. Numerous Security methods have been suggested to deliver safety resolutions besides numerous threats to the Cross-layer modification techniques in Wireless sensor networks. In this paper we overview the existing schemes for the security of cross-layer design in wireless sensor networks. The proposed Security model will provide more security between sensor nodes and the base station in wireless sensor network.Security is important for the success of the wireless sensor network because the data collected are often sensitive and the network is particularly vulnerable. In the cross-layer design, constraints are substituted between changed layers to protect the well-organized use of energy. In this paper, we propose a secure security model that is based on cross-layer design. It uses a cross-layer optimization Machine. Reproduction consequences confirm that our proposed safety model better in many situations and in unpromising violence-disposed to the situation.

***Keywords*--**Security, energy Efficiency, Security Frameworks key management, Wireless Sensor Network.

I. INTRODUCTION

In obsolete broadcast systems, the Open Systems Interconnection (OSI) covered building has been extensively accepted and has helped numerous communications to organization stealthy in the past; however, growing wireless networks of nowadays are extremely exciting to this design idea. The layered construction expresses a mountain of procedure layers in which each layer function within its precise utility and front line and thus permitting dissimilarities to the fundamental expertise at each layer deprived ofunexpected the essential to modification the complete system construction [1][2]. There is additional problematic to provide awell-organized and accessible security explanation. Themainfundamentals of Wireless Sensor Networks are the sensor nodes and the base stations. In fact, they can be preoccupied as the “sensing cells” and the “brain” of the network, constantly. Typically, sensors nodes are organized in anelectedexpanse by aspecialist and then, robotically form a network finished wirelessCommunications.Two main security challenges in secure data aggregation are confidentiality and integrity of data. While encryption is traditionally used to provide end to end confidentiality in wireless sensor network, the aggregators in a secure data aggregation scenario need to decrypt the encrypted data to perform aggregation. This exposes the plaintext at the aggregators, making the data vulnerable to attacks from an adversary. Similarly an aggregator can inject false data into the aggregate and make the base station accept false data. Thus, while data aggregation improves energy efficiency of a network, it complicates the existing security challenges.In wireless sensor network it is necessary to allow only specific sensor node to access your wireless sensor network**.** Each sensor node that is intelligent to interconnect with a wireless sensor network is allotted an exclusive Media Access Control address. Wireless routers regularly have a machinery to permit only devices with specific media access control reports to admission to the wireless sensor network. Little positioning charges of sensor nodes variety wireless sensor networks nice-looking to handlers. Distribution of sensor nodes in exposed situation also provides attacker the trappings to promotion occurrences on the wireless sensor network [3][4].The design defects in the sanctuary apparatuses of the 802.11. Average also gives growth to a number of probable occurrences, both submissive and dynamic. These occurrences empower impostors to overhear on, or interfere with, wireless transmissions. Sensor nodes are fast, mountable, low dynamism effectual and extremely circulated in exposed atmosphere so there is safekeeping is essential for superiority of provision in wireless sensor network [5]. A cross-layer design approach is introduced in Lazos and Poovendran where a key management mechanism in wireless multicast is proposed. With this approach, secret keys to valid group members are deployed in an energy-efficient way. Authors considered the physical and network layer in combination. There is need of security solution for cross layer design in wireless sensor network because there is one layer can communicate with another layer non-adjacently. Wi-Fi protected access should be used for encryption of data in wireless sensor networks. In this paper we planned a safetyresolution that will affordsafety to coatings in Wireless Sensor Networks [6] [7].

II. REQUIREMENTS OF SECURITY IN WIRELESS SENSOR NETWORKs

Security is a large apprehension when Wireless Sensor Networks are positioned for unusual claims such as fighting and healthcare. Owed to their exclusive arrivals, outdated safe keeping approaches of computer networks would be useless for wireless sensor networks. Hence, deficiency of security apparatuses would origin impositions near those networks. These impositions need to be distinguished and indication approaches should be functional. Two main security encounters in protected data accumulation are privacy and truthfulness of statistics. While encryption is conventionally used to deliver end to end discretion in WSNs, the aggregators in a protected data accumulation situation need to decrypt the translated statistics to achieve accumulation. Maximum of Wireless Sensor Networks are used to intelligence, assemble, and procedure delicate evidence. Statistics discretion and truthfulness is one of the significant purposes in such belongings. This sympathetic of objective can be accomplished by manipulative approximately sort of security apparatus particularly permitting security apparatus in direction-finding protocol. Significant requirement of any network is to security,privacy, truthfulness, and obtain ability.Explanations for appreciative cross layer security method and to name some we have dissimilar necessities and facilities of requests dominion, cross layer interruption discovery, discovery of self-interested protuberance and non-dismissed security.

Wireless Sensor Network contains of spatially disseminated independent instruments to monitor conservation environments of the ground. The expansion of wireless sensor networks was interested by martial submissions such as battle ground observation. Wireless Sensor Networks are organized at dangerous at comparable observation, checking, airfields, battle ground requests here after safe guarding Wireless Sensor Networks is a very stimulating duty. The foremost requests are measured as the normal security supplies, which are as the following:

(a) Data Confidentiality
(b) Data Truthfulness
(c) Data Availability
(d) Freshness
(e) Self-Organization
(f) Secure Management
(g) Quality of Service

(a) Data Confidentiality

Data confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft. Confidentiality has to do with the privacy of information, including authorizations to view, share, and use it.

(b) DataTruthfulness

Data truthfulness enforces the service provider to truthfully collect and process real data. The essence of TPDM is to first synchronize data processing and signature verification into the same cipher text space, and then to tightly integrate data processing with outcome verification via the homomorphic properties.

(c) Data Availability

Data availability is a term used by some computer storage manufacturers and storage service providers. Data availability is the process of ensuring that data is available to end users and applications, when and where they need it. It defines the degree or extent to which data is readily usable along with the necessary Information Technology and management procedures, tools and technologies required to enable, manage and continue to make data available.

(d) Freshness

One of the many attacks boosted in inconsistency of sensor networks is the message replay attack where an adversary may capture messages exchanged between nodes and repetition them later to cause confusion to the network. Data cleanness impartial safe guards that communications are fresh, meaning that they obey in a message ordering and have not been reused. To accomplish cleanness, network protocols must be considered in a way to recognize replacement packages and throw away them stopping probable is calculation.

(e) Self-Organization

Each node in a wireless sensor networks should be self-organizing and self-healing. This feature of a wireless sensor networks also poses a great challenge to security. The dynamic nature of a wireless sensor networks makes it sometimes impossible to deploy any pre-installed shared key instrument among the nodes and the base station. A number of key pre-distribution schemes have been proposed in the context of symmetric encryption. However, for application of public-key cryptographic techniques an efficient mechanism for key-distribution is very much important. It is anticipated that the nodes in a wireless sensor networks self-organize among themselves not only for multi-hop routing but also to takeout key management and developing faithrelatives[13][14].

(f) Secure Management

Management is required in every system that is constituted from multi-components and handles profoundmaterial. In the case of sensor networks, we need safe management on base station level; since sensor nodes communication ends up at the base station, issues like key delivery to sensor nodes in order to found encryption and routing information need secure management. Furthermore, clustering requires secure management as well, since each group of nodes may include a large number of nodes that need to be authentic with each other and exchange data in a safe manner. In addition, clustering in each sensor network can change dynamically and fast. Therefore, protected protocols for collectionadministration are mandatory for adding and eliminating associates and confirmingstatistics from assemblies of nodes.

(g) Quality of Service

Quality of Service impartial is a large annoyance to security. And when we are talking around sensor systems with all the boundaries they have, quality of service develops even more controlled. Safety instrument sobligation be insubstantial so that the above caused for example by encryption must be minimalized and not disturb the concert of the network. Concert and superiority in sensor networks comprise the appropriate transfer of statistics to stop for example broadcast of contamination and the correctness with which the data conveyed match what is really happening in their situation.

III. PROPOSED SECURITY MODEL

Cross-Layer Design (CLD) is a co-operation amongnumerouslayers. Cross layer design permit communication between layers non-adjacently. We planned a Security model for CLD in wireless sensor network. Fig.1 shown a cross-layer security model for wireless sensor network. In this cross-layer security model we are using a security filter between cross-layer design and cross-layer optimization handler. When sensor node want to send sense data to base station then first check whether channel free or not if channel is free then sense data forward to security filter. Security filter check the sense data and give a token (time slot) to packet node. After receiving token from security filter sensor node forward sense data to Cross layer optimization handler (CLOH).Cross layer optimization handler is used for merging layers for communication non-adjacently. Cross layer optimization handler Combine the resources and provide communication between layers [15].

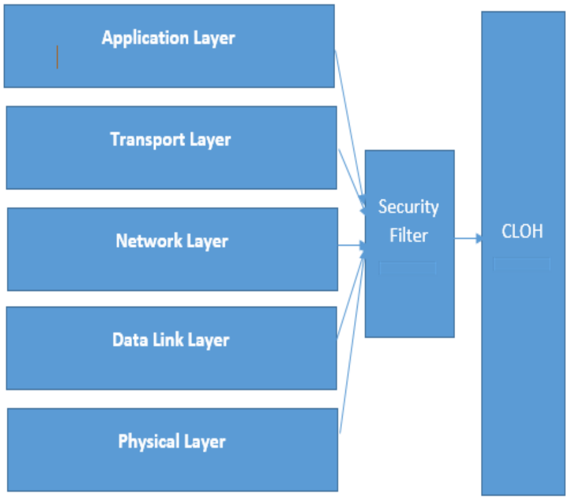

Fig1. Proposed Security Model for Cross layer design

Notations used:

SF–Security Filter
P_N _Packets node
CLOH -Cross layer Optimization Handler
T_s-Time Slot
Ch–Channel
BS-Base Station

Algorithm for security of data

```
1.  If Sensor node want to send data to base station
2.  Check Channel Ch whether it is free or not
3.  If Ch=0 then set Ch=$P_N$
4.  Set SF =$P_N$
5.  Set $P_N$=$T_S$
6.  $P_N$ dispatchfrom SF to CLOH buffer
7.  CLOH Check Ch is free or not
8.  If Ch=0 then
9.  Dispatch $P_N$ from CLOH to BS
10. Repeat Step 1 to 9
```

IV. RELATED WORK

Wireless sensor networks has numerous solicitations such as extensive extent investigation for boundaries safety, checking temperature, comprehensive, and compression in an agreed expanse many investigators intentional the security matters in WSNs. There is a significant quantity of investigations in the works that deliberate Wireless Sensor Networks knowledge in universal [1][7].The complete collected works examination of safety subjects in cross-layer deliberate in [8][10]. Djallel Eddine Boubiche et al. [8] have planned a new delicate watermarking based protocol to reservation the data accumulation honesty in varied WSN. Proposed procedure is vitality effectual and it progresses the statistics accumulation procedure on the assorted nodes and improves the statistics accumulation accurateness. Geethapriya Thamilarasu et al. [9] have explore the impression of cross-layer practices on safety and network recital using two different types of cross-layer edifices based on shortest communication between layers and using shared database model. Both enterprise performed improved in positions of sophisticated system stability and lower employment complexity. Pedro Pinto, Antonio Pinto et al. [10] have planned a novel cross-layer admission control (CLAC) instrument to enhance the network performance and increase energy efficiency of a wireless sensor networks, by avoiding the transmission of possibly useless packages.CLAC augments the inclusive network routine by cumulative the quantity of valuablepackages [16].

V. PERFORMANCE ANALYSIS OF PROPOSED SECURITY MODEL

We develop a simulation environment to evaluate the efficiency of security model. For this purpose we are using QualNet 5.0.2 simulation modeling tool.The performance of proposed Security model is verified with cross layer design in the experimentation, the sensor nodes in WSNs are disseminatederratically in the 100m * 100m area. We are using some limitations in this reproduction that are shown in Table 1.

Table 1: Simulation Parameters

Parameter	Value
Source Sensor nodes	1,2,3,4,5,6,7,8,9,10
Destinationnode(Base Station)	11
Packets Send	40000
Terrain Range	100m x 100m
No. of nodes	10
Frequencies	2.4GHz
Traffic Type	CBR
Channel Type	Wireless channel
Protocols	AODV

In this simulation environment (Fig. 2) Source sensor nodes 1,2,3,4,5,6,7,8,9,10 are co-operately pass their data to the destination node 11 (BaseStation). Running simulation is shown in Fig. 3.In running simulation sensor nodes are sending packets to destination node 11(Base Station).In Fig.4 shown the result, total packets received by destination sensor node 11 or Base Station. Total packets send by source sensor nodes was 4000.By using Security model, Base station received 100% packets from sensor nodes 1, 2,3,4,5,6,7,8,9,10.Base Station received 4000 packets from Source sensor nodes.

By implementing security model with cross layer design we are getting 100% secure data at Base Station.

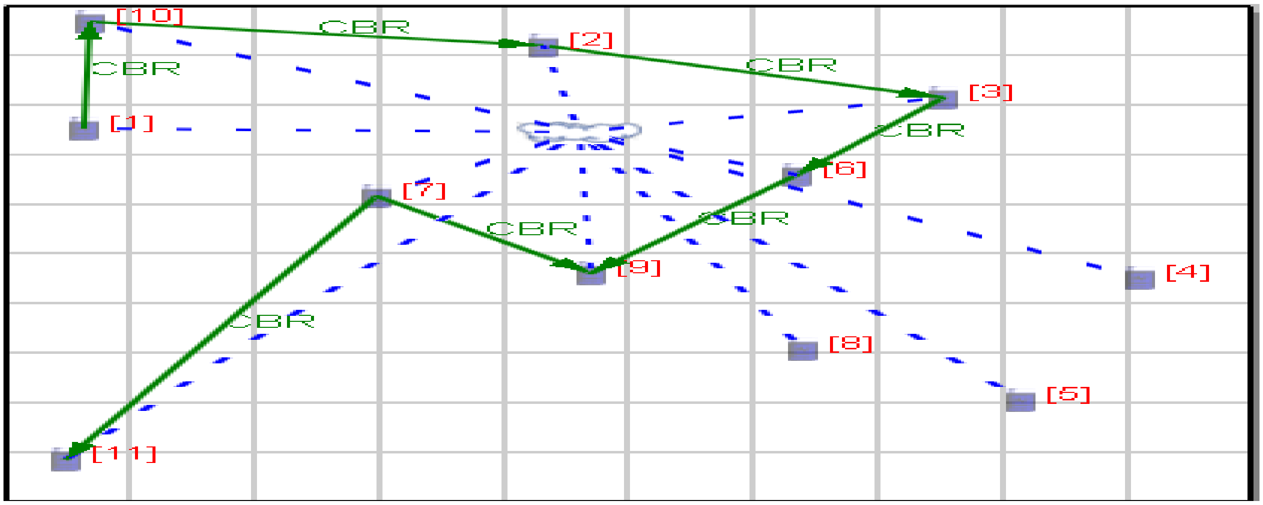

Fig.2 Simulation Setup

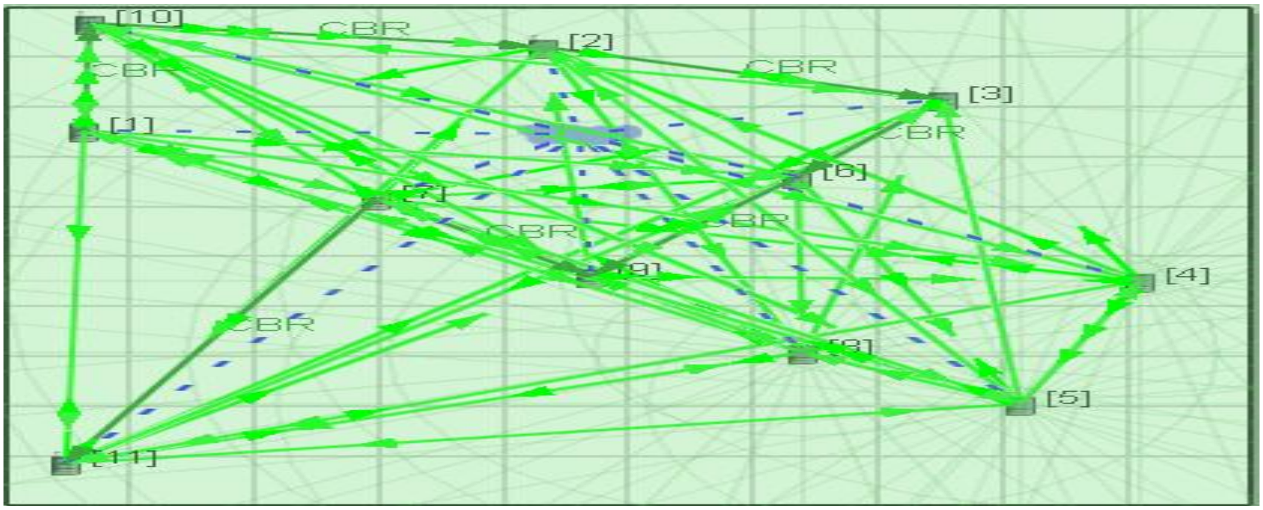

Fig.3 Running Simulation

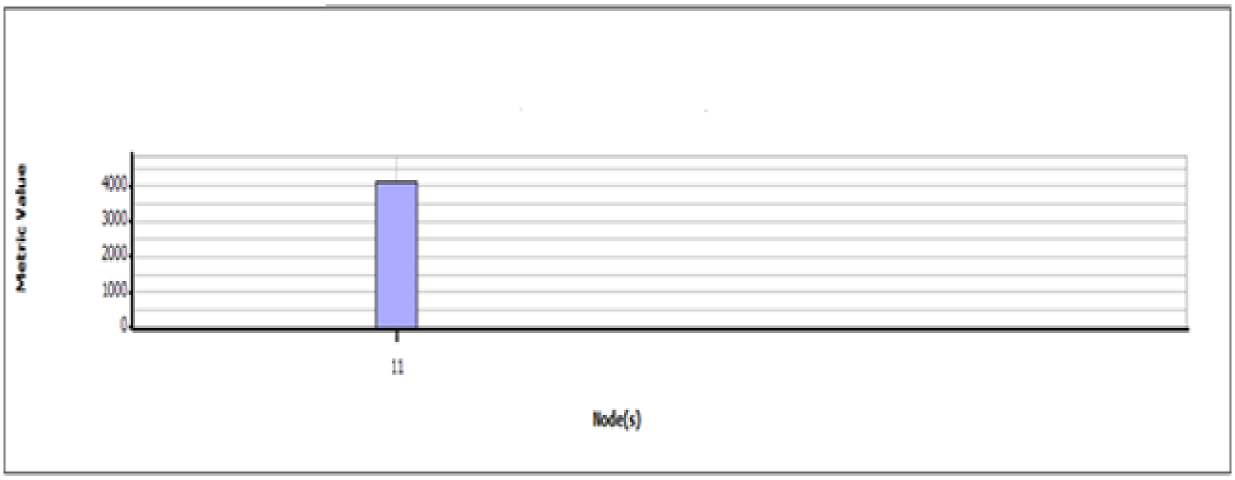

Fig.4 Total packets received by Base Station

VI. CONCLUSION

In this paper a novel method of safety explanation for Wireless Sensor Networks is obtainable. In the current centuries, Wireless Sensor Networks protection has been intellectual to application the considerations of a number of investigators about the ecosphere. Wireless networks are frequently supplementary susceptible to numerous safety pressures as the untraced announcement intermediate is more vulnerable to security occurrences than those of the conducted transmission intermediate. Security is a significant constraint and confuses sufficient to set up in dissimilar fields of Wireless Sensor Network. In this paper we proposed a new security model for cross layer design in wireless sensor networks. The planned security model is very valuable for dissimilar requests of wireless sensor networks such as armed claim, Health request and manufacturing monitoring application and so on. In this paper we estimate presentation of projected security model by using Qualnet 5.0.2 Simulator instrument and find that planned security model provide 100% security between layers.

REFERENCES

[1] Ameer Ahmed Abbasi, Mohamed Younis, “A survey on clustering algorithms for wireless sensor networks", Computer communication 30(2007)2826-28410.

[2] J. N. Al-Karaki and A. E. Kamal, “Routing Techniques in Wireless Sensor Networks: A Survey”, IEEE Wireless Communication Vol.11, No.6, Dec.2004, pp. 6-28.

[3] Amir Sepasi Zahmati and Bahman Abolhassani, “EPMPLCS: An Efficient Power Management Protocol with Limited Cluster Size for Wireless Sensor Networks”, Proc. 27th International Conference on Distributed Computing Systems (ICDCS 2007), submitted for publication.

[4] W. B. Heinzelman et al., “An Application-Specific Protocol Architecture for Wireless Micro sensor Networks,” IEEE Transactions on Wireless Communications Volume 1, No. 4, Oct 2002, pp.660 - 670.

[5] W. R. Heinemann, A. Chandrakasan, and H. Balkrishnan, “Energy-Efficient Communication Protocol for Wireless Micro sensor Networks”, in Proceedings of 33rd Hawaii International Conference on System Science, Vol. 2, Jan. 2000, pp.1-10.

[6] Amir Sepasi Zahmati,Bahman Abolhassani,Ali Asghar Behesti Shirazi and Ali Shojaee Bakhtiari, ”An Energy-Efficient protocol with Static clustering for Wireless Sensor Network", proceedings of world academy of science, Engineering and Technology volume 22 July 2007 ISSN 1307-6884.

[7] SoheilGhiasi, Ankur Srivastava, Xiaojian Yang, and Majid Sarrafzadeh, “Optimal Energy Aware Clustering in Sensor Networks”, SENSORS Journal, Vol. 2, No. 7, 2002, pp. 258-269.

[8] DjallelEddineBoubiche, Sabrina Boubiche, AzeddineBilami, “A Cross-Layer Watermarking-Based Mechanism for Data Aggregation Integrity in

Heterogeneous WSNs."IEEE Communications Letters, Vol.19.No.5, May 2015.

[9] Geethapriya Thamilarasu, Ramalingam Sridhar, "Exploring Cross-layer techniques for Security: Challenges and Opportunities in Wireless Networks.", Proc.IEEE 2007.

[10] Pedro Pinto, Antonio Pinto, Manuel Ricardo, "Cross-Layer Admission Control to Enhance theSupport of Real-time Applications in WSN", IEEE Sensors Journal, Vol.X.No.X, XX.

[11] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.

[12] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp.407-411.

[13] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS2006.

[14] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at,http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf.

[15] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for Sensor Networks", Wireless Networks, vol. 8, no.5, 2002, pp. 521-534.

[16] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.

[17] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M.,and Tuan, T., "PicoRadios for wireless sensor networks: the nextchallenge in ultra-low power design" 2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 –201.

Author Profile

Dr.Rakesh Kumar Saini received the MCA degree from UPTU, Lucknow, India in 2005 and M.Tech (Computer Science and Engineering) degree from UTU, Dehradun, India in 2012 and PhD from DIT University, Dehradun, India in 2017. He is having more than 14 Years of teaching experience. He is author of around 10 books. His research interests include cross-layer modification, Energy-Efficiency and water quality monitoring in Wireless Sensor Network.

Mr. Naveen Kumar, Assistant Professor in Department of Computer Science and Engineering. At DIT university Dehradun (U.K.).He is having 12 Year + teaching and research experience. The Research Area is Wireless Sensor Network and Data Mining.