ISSN:0975-9646

Secure Data Packet of Cluster Head and Base Station in Wireless Sensor Networks

Abdo Saif Mohammed,
Department of Electronics and Communication
Sri Jayachamarajendra Colleges of Engineering
Mysore, Karnataka, India.

M.N.Shanmukhaswamy
Department of Electronics and Communication
Sri Jayachamarajendra Colleges of Engineering,
Mysore, Karnataka, India.

Abstract-LEACH in wireless sensor networks (WSNs) achieves good performance with reserving energy consumption and decreasing system delay. LEACH protocol does not consider a security issue for ensuring the protection of the network. So the security in LEACH is a complicated task. were we improved the LEACH protocol called a novel algorithm to select cluster heads with highest and balanced energy in wireless sensor networks to choose the cluster head with the highest energy. Were the cluster heads gathered data from the surrounding nodes and send it to the base station. But this data collecting from surrounding area to the cluster heads and base station without consider about security. In this paper, we improved a novel algorithm to select cluster heads with highest and balanced energy in wireless sensor networks with authentication protocol to protect our previous work and network from attackers. This protocol uses RSA algorithms to secure packet during send to both cluster heads and base station. The results of simulation not only prolong the lifetime of wireless sensor networks, but also enhance routing security strongly.

1. INTRODUCTION

The key distribution is one method to secure a wireless sensor networks, however, most of studied recently in WSN proposed a key distribution is the best one during using cryptographic to any network. LEACH radically depends on the creation of clusters and distribution the information between the clusters, normal nodes and the base stations through rotated the nodes periodically on the basis of energy. So it will be easy to penetrate the opponents of information transmitted from one point to another, and for this reason, most of the studies have focused to protection this type of protocols. For your information there are other protocols have the ability to making it harder for an adversary to identify the routing elements and compromise them [3]. But the protocols are based on clusters has proved its efficiency in terms of energy conservation and extend the life of the network. There is a challenge to adding security to LEACH protocols, because the cluster heads randomly selected without advance information to the base station. makes the key distribution solutions is difficulty, but adding security to our work that improve to LEACH ,it is very easy ,because there is advance information to the base station about witch node it will became as cluster and witch ordinary nodes.

2. RELATED WORKS

In [1] the authors suggested a way there is no need specific hardware and clock synchronization due to use encryption concepts such as digital signature. Where each node authentication by using digital Signature (RSA). Received a node in the destination node Verified and if the digital signature is incorrect information about that is sent to the sender node using DATA_ACK.

Author [2], described MIN-RC to enhance Leach-C protocol, were they used method of adaptive round-control to enhance the energy consumed during the round of WSNs.

The authors suggested TinySec [3], which is based on the implementation of the security layer link on the level of packets. This proposed provides a way to authenticating and encrypting packets, focus on the use of an initialization vector to improve the encryption technology, but does not produce a new locking mechanism and instead apply security on the one-hop level. In the implementation of the provided work, Researchers are spread the key across network.

Authors suggested TinySec [4], to implementation link layer security to secure the packets. This proposed provides packets with authenticating and encrypting, this protocol focuses on the use of an initialization vector to improve the encryption technology.

Author attempts to use public key encryption systems in wireless sensor networks began, and suggested a TinyPK [5] protocol with to take advantage of the public keys based on TinySec.

Authors [6] proposed a new protocol improve to TinySec with lower energy consumption and higher security than TinySec.

The authors [7] suggest using the benefits of the symmetric and asymmetric cryptographic operations to improve wireless sensor networks security.

Author [8]; attempt to protect CHs from attacks by using security to WSNs.

Authors [9], proposed to provides energy-efficient and secure communication on the network layer .For key distribution and authentication, securing the routing mechanism.

Ye Xiao Lin et al [10] said the RSA is a safe and easy algorithm to be implemented and the most common used Asymmetric algorithm; it is based on the factorization of

large number. RSA not only used for data encryption and authentication.

RC5 is a block cipher notable for its simplicity. Invented by Ron Rivest and analyzed in the laboratories of RSA. It has a word size variable, a variable length of the secret key and variable number of rounds. RC5 is its heavy use of data-dependent rotations - rotations are random variables dependent on the input data, and they are not predetermined values as said by Ali, A [11].

In [12], the authors compare DD and LEACH protocols with respect to energy consumption and security service, confidentiality, using ElGamal, RSA, ECC and RC5 crypto systems.

It is found that ECC offers better security features and can withstand attacks when compared to other algorithms, but ECC consumes more energy compared to RSA and ElGamal asymmetric algorithms.

3. SECURITY ANALYSES

Wireless sensor network have many application, such as, environment monitoring, military applications, burglar alarms, hospitals, etc and any kind of activity. So the WSN consider the security is an important issue to implement its application. Where these application dependent on sensor nodes that have limited energy ,therefore, our ability to add the classic security mechanisms to the sensors nodes hardware and software, we have decided to come up with new techniques to avoid an intruder to steal or manipulate data that can cause disaster. The goals of the any secure system is to provide confidentiality, integrity and availability (CIA) for the data, protecting information from unauthorized access, use, modification, disruption, disclosure or destruction [1]. Usually use cryptographic functions to ensure this, but due to limited memory and energy of sensor nodes, most of these cryptographic functions cannot be directly converted from traditional security systems to WSN. In addition , as happened in the early days of the Internet, the protocols of clustering algorithms are not consider about the security and they are insecure. And therefore we have to think of new mechanisms for adding a layer of security to our sensor nodes. many researches Some research have been studying in WSN and some of its focus on implemented cryptographic methods. Such as, TinyOS 1.0 on a unit called TinySec layer that provides a link security architecture. If we use the new TinyOS 2.0 or TinyOS 2.1, we found the development of a new application for AES for MICAz on TinyOS. however, they didn't give the good simulator to TOSSIM problem to emulate the behavior of the cryptographic module.

4. ATTACK IN WSN

Security attacks can be classified into two major categories: passive and active. In a passive attack the intruder does not convey anything to try to confuse the network, and it's just stand and listen to the other what they send. This type of attacks in an attempt to break the premise of confidentiality, because they are listening to the conversation that has not been addressed to him.

This type of attack is more dangerous and can pose a threat to the confidentiality, integrity and availability of the sensor nodes. Radio frequency (RF) of wireless sensor network uses to transfer of the medium-term parking. This way, make easier thinking of intruder to tamp the passive attacks, because any node that antenna correctly can get this information sent by others. f the behaves of the sensor as a legitimate node, will get any packet has different purpose for the specific purpose and the sensor will remove out this packet. But if there is illegal node within the network, it will hide itself to listen the medium to gather all information transmitted among the nodes. But the difficult detecting and dangerous type of attack is Passive attacks if the data and there is no authentication or cipher, and these can be easily carried out with dangerous impact. Two categories of passive attacks eavesdropping and traffic analysis. Eavesdropping use to listening the medium and collect information about packets in order to break the privacy or confidentiality of sensor node. For example, when we are watching any kind of activity through sensors can eavesdropping attack remember this private information. On the contrary, from the analysis of traffic in an attempt to find out whether there is any pattern within the network. Active attacks can be grouped into: physical, masquerade, replay; edit the message, and denial of service and misconduct. Fig.1 show us a better description [8].

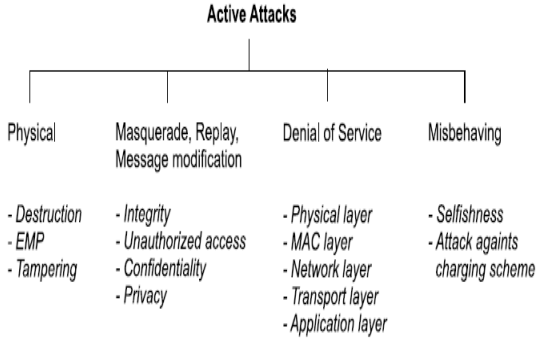

Fig. 1:Active Attacks

Psychical attacks occur when malicious access to psychological device. If this happens, the attacker can damage device and kill the sensor. In the case of the network may not support fault-tolerant award pay for this attack could be even higher than that. Can be hidden enemy within the network, receive messages of cluster algorithm and then modify this messages and return it to the network. If the malicious node injection to cluster formation protocol it may modify in one's own way to achieve its goals. This is used as a masquerade, and modifies the message and replay attack. Denial of service (DoS) includes a broad kind of attacks and their attempt is to make a resource unavailable to its intended users. Denial of service can be made at any layer, for example, in the psychical layer we can cause a DOS-in a sensor with just emits another signal with the same frequency near the node. This causes a lot of noise in the carrier, so the receiving node cannot get the information

correctly. Various DoS can be done successful in the link layer depending on the medium access control (MAC) that the sensors have implemented. MAC for TinyOS is just CSMA, unlike standard Wi-Fi (802.11b/g) uses CSMA/CA and RTS/CTS packets to solve the problem of hidden terminals and exposed terminals. Regarding RTS/CTS is not available in TinyOS the problem of the hidden terminal is always present.

Thus there node that are ready to forward to the node B because it does not see malicious Station C (according to CSMA) and the sensor C can always forward and caused a collision in the node B, B will never receive the signal of node A. In this case, the node C has the resources (Node B) always for him, and at the same time node A can never get to the source. Can also be included this latter behavior as misbehaving category. Moreover, continuous retransmission of the packet node A can also deplete the battery of node. At the network layer, where clustering algorithms works as illegitimate node can reject the message or change it to follow the algorithm and avoid a node to communicate with others, and form correctly clusters . At the end, in the transport layer mechanism of ACK and messages can be manipulated to jam some nodes.

5. LEACH ALGORITHM

LEACH algorithm was described in Chapter 2; therefore here we are analyze the security threats and possible attacks to carry out in the clustering algorithm.

6. HELLO FLOOD ATTACK

Then the ordinary nodes must be affiliated with only one cluster head based on some discriminatory parameters with respect to signal, distance or the energy level. The original algorithm of LEACH selects the cluster head with best signal strength. This fact can lead to malicious (a laptop-attacker with a power antenna) to emit always signal strength and which are the best of any node. Thus, each sensor in the network, and we will try to associate to this node. But not all motes will associate with the distribution of the intruder, because the radio signal of wireless is not strong, such as a laptop, and they cannot reach to adversary node.

These packets lost may involve network to stay in the inconsient case. In the other meaning, it may cause a DoS. In this implementation they did not used signal strength to associate the best node. Instead of these, but they used as discriminatory factor of distance. Because of them distribution is placed on the grill reform (and they know the distance between nodes) cannot be carried out the Hello attack. On the other hand this fixed topology does not give them the flexibility to design those networks.

7. SYBIL ATTACK

Another choice without causing a DoS to spread malicious nodes strategically in order to transfer all the data in the sensor network to the illegitimate motes. Can be easy to face this issue that LEACH selects in each round a cluster head that has not been pre-selected. In this scenario the Sybil attack comes up. A single node presents multiple identities in Sybil attack [10]. And therefore, the adversary can changes its identity in each round to appear as a new node to the rest of the network, and therefore can be chosen again. they can transfer all the data from the network to sensor nodes and then analyze the traffic, which is in plain text or make a wormhole to respond to data in another point.

8. OTHER ATTACKS

The implementation of LEACH stressed that the algorithm in the right way. As a result of that, if the nodes do not follow the normal flow of network algorithm may lead to an inconsistent state. Such as, if we have an adversary that is cluster head and receive all the data from the ordinary and sub cluster nodes, but does not send the data collection to the sink, this will be waiting until they receive a package from all CH (causing a DoS). Another selection is to forward a messages such as associates when it is not the right time in the flow of the algorithm. In the case of the associative messages, The cluster head receives all packet and allocate slot in the TDMA shadily received node, without checking if the node is already in the schedule. If a malicious node sends a burst of associative messages, and this could lead to a buffer overflow. Even if the algorithm achieved without unnecessary nodes in the schedule TDMA, the adversary can always uses the Sybil attack to change its identity.

9. RSA ALGORITHM

Considering WSN continuous monitoring, use the RSA algorithm to Secure the network. RSA include tow keys one as public key and second as private key is generated in every node. In this proposed during the formation of the cluster heads and organize it in rounds we built a table of keys in the base station; this table is generate public key and private keys at all the nodes. Base station having both location of all the other nodes and table of keys in routing table, routing table can contact on the three main cluster heads with a public key and private keys generation. The RSA security is inherent with the difficulty of factoring large numbers.RSA encryption and decryption algorithms require exponential process and single nodular. Coefficient determines the size cipher security force.RSA is the following components [14].

Key generation:

- Select random prime numbers p and q, and check that p != q
- Compute modulus n = p*q
- phi= (p - 1)(q - 1)
- Select public exponent e, 1 < e <phi
- Compute private exponent d = e^-1 mod phi.
- Public key is {n, e}, private key is d
- Encryption: c =m^e mod n , decryption: m =c^d mod n

The public key consists of {e, n} and private key consists of {d, n}. Suppose first user send a message M with public key and second user receive a message by using C = M^e mod n and transmits C by using M = C^d mod n.

10. PROPOSED WORK

We proposed to secure our previous work [15] that improve to LEACH protocol, we used RSA algorithm to secure our work to insurance safety packet reach to CH and BS. In wireless sensor networks, there are a number of sensor nodes and a base station (BS).Where we sort the sensor nodes as descending on accounting to the energy and we select the three nodes with highest energy as a cluster heads and divided the remaining nodes to sub cluster heads and ordinary nodes .In our work every nodes have pri information about which one become cluster head, sub cluster and ordinary nodes. So uses CSMA is limited in our work and RSA algorithm is suitable for encrypting and decryption our proposed work.

10.1. Security vulnerabilities

In WSNs our work is vulnerable to a number of security attacks [13], including jamming, replay, etc. However, because the data aggregation and routing in our work dependence on CHs to collect information from ordinary nodes and Process it and send it to base station. So most of the attackers focus on penetrating CHs in order to control the transfer of information from and to CHs to the base station.

10.2. Crypto systems

A crypto system is an indispensable tool for protecting information in any protocols, used for encryption and decryption of messages or a package using cryptographic algorithms. There are a many types of cryptographic technique such as stream ciphers, block ciphers and hash functions. but most of this way used one key for both encoding and decoding; they can have separate keys for encoding and decoding with pri information about secret key, during a crypto system. also There are other types of algorithms such as symmetric and asymmetric. where symmetric uses single key for both encryption and decryption and asymmetric use different keys for encryption and decryption respectively. Public key is used for encryption and its related private key is used for decryption. So we selected RSA algorithms, because it suitable for encrypting our small packet.

10.3. Adding Security to our previous work:

This proposed focus in secure a WSN by prevent illegitimate CHs from participating in the network. This access control can keep a lot of operations on the network, unless the penetrating legitimate compromised. Our proposed implemented by using RSA cryptographic mechanisms to secure the data packet send to the cluster heads or base station in WSNs [15]. Our proposed [15] and LEACH algorithm works in rounds. Each round is classified into two phases:

- Setup phase
- Steady phase

10.3.1. Set-Up Phase

- CH ⟹ N: id
- ni ⟶ CH: id > CH: idni , idCH ,crc, join_req
- CH ⟹ N: idCH ,(… ,(idni , Tni)…) , crc ,sched

10.3.2. Steady State Phase

- ni ⟶ CH : idCH ,ci , crc

Where,

ci = E (mi, Pk) = ci = mi ^e mod n

Pk= {n, e}

Pv=d

(Pk, Pv) = KeyGen(x)

KeyGen= Key generation:

- Select random prime numbers p and q, and check that p != q
- Compute modulus n = p*q
- phi= (p - 1)(q - 1)
- Select public exponent e, 1 < e <phi
- Compute private exponent d = e^-1 mod phi.
- Public key is {n, e}, private key is d

At Cluster heads after receiving data from all the sensor nodes decrypt the data to obtain the original data.

mi =Dec(C, Pv) = mi = C ^d mod n

Where,

C=ci, Pv, ci+1, Pv, ci+2, Pv, ci+n-1, Pv

- CH ⟶ BS: idCH , idBS, (c1,Pk,c2,Pk, …,ci, Pk), crc

At Base Station after receiving data from all the cluster heads, base station decrypt the data to obtain the original data.

mi =Dec(C1, Pv,c2,Pv,…,ci,Pv) = mi = C ^d mod n

The symbol used in proposed algorithm denotes:

CH, ni, BS: Cluster Head, ordinary node, base station

N: Set of all nodes in the network

Adv, join_req, sched: String identifiers for message types

Crc: Cyclic redundancy check

mi, ci: plaintext, cipher text

x: Security Parameter

idni, idCH, idBS: Nodes ni, CH, BS id's respectively

Tni: A node id & its active slot in the clusters TDMA schedule

⟶: Uncast transmission

⟹: Broadcast transmission

11. SIMULATION RESULTS

The proposed work is simulated using Mat lab which consists of 100 sensors nodes, where 51 nodes act as ordinary nodes and 49 act as cluster heads, a base station consists routing table, this table is generating public key and private keys at all the nodes. The cluster heads send his information with encrypted by using its public key to the base station and the destination receives his encrypted information from base station and decrypted it by using its private key as shown in fig.3 and fig.5.

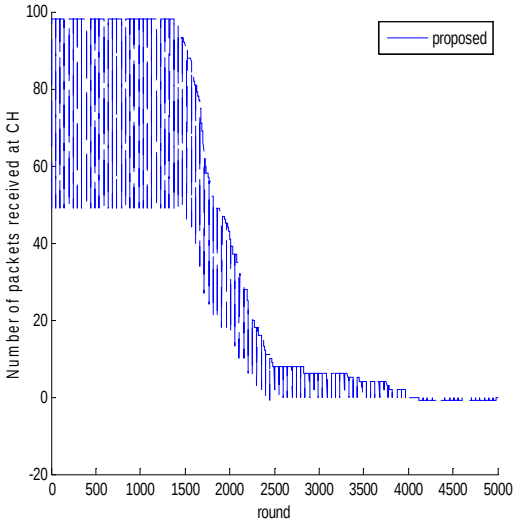

Fig .2: Number of packet received at the CH without security

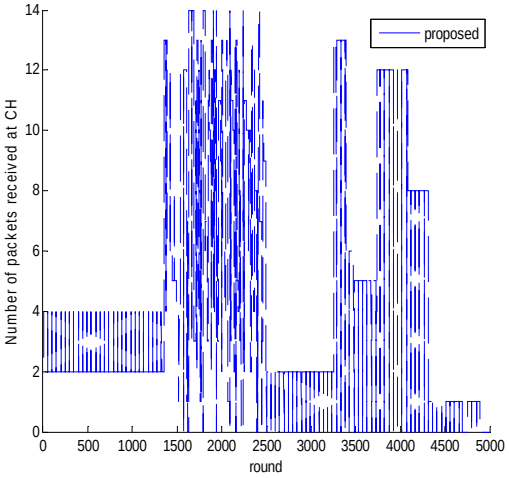

Fig .3: Number of packet received at the CH with security

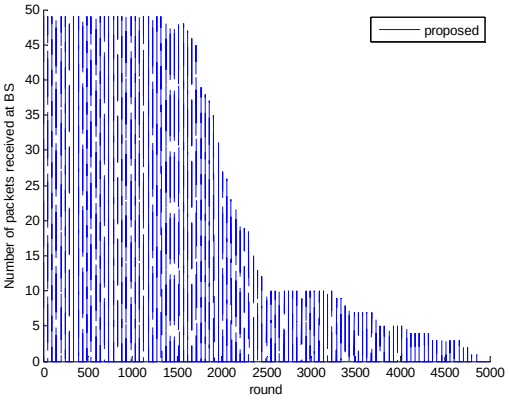

Fig .4: Number of packet received at the BS without security

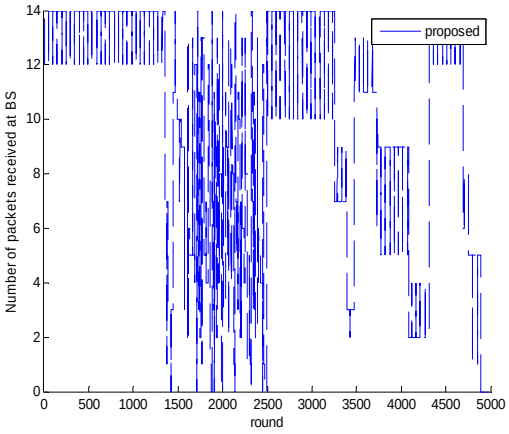

Fig .5: Number of packet received at the BS with security

12. CONCLUSION

In this paper, we look at RSA to secure our proposed work in routing protocols, which can have a significant impact on the reliability and energy dissipation of these networks. Proposed amendment worked with cryptographic protection against attacks from abroad and prevents an intruder from becoming a CH or by injection of fake sensing data in the network. This is proposed making the base station can receive any information with sufficiently high power from any node in the network.

ACKNOWLEDGEMENTS

The authors wish to acknowledge J.S.S Research Foundation, S.J.C.E Technical institutions campus, Mysore, Karnataka, India for all the facilities provided for this research work.

REFERENCES

[1] .Er. Kumar, Saurabh, Sukhpreet"Providing Security in Data Aggregation using RSA Algorithm" International Journal of Computers & Technology.

[2]. Mahendra S. Thakare "Security of Cluster Based Wireless Sensor Routing" International Journal of Latest Trends in Engineering and Technology (IJLTET).

[3] C. Karlof, N. Sastry, D. Wagner. TinySec: Link Layer Security Architecture for Wireless Sensor Networks. Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys '04), Baltimore, Maryland, November 2004, pp. 162-175.

[4] C. Karlof, N. Sastry, D. Wagner. TinySec: Link Layer Security Architecture for Wireless Sensor Networks. Proceedings of the 2nd ACM Conference on Embedded Networked Sensor Systems (SenSys '04), Baltimore, Maryland, November 2004, pp. 162-175.

[5] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, P. Kruus.TinyPK: Securing Sensor Networks with Public Key Technology. Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04), Washington, DC, USA, October 2004, pp. 59-64.

[6] M. Luck, G. Mezzour, A. Perrig, V. Gligor. MiniSec: A Secure Sensor Network Communication Architecture. Proceedings of the 6th international conference on Information Processing in Sensor Networks (IPSN '07), Cambridge, Massachusetts,USA, April 2007, pp. 479-488.

[7]. Watfa, M., El-Ghali, M. & Halabi, H. 2008, 'A scalable security protocol for wireless sensor networks', International Conference on security and management (SAM '08), 2008.

[8] A. Modirkhazeni, N. Ithnin and O. Ibrahim, “Empirical Study on Secure Routing Protocols in Wireless Sensor Networks,” International Journal of Advancements in Computing Technology, Vol. 2, No. 5, 2010, pp. 25-41.

[9] J. Ibriq and I. Mahgoub, “A secure hierarchical routing protocol for wireless sensor networks,” In: Proc. 10th IEEE International Conference on Communication Systems, 2006,pp. 1-6.

[10] Yi Xiaolin; Chen Nanzhong; Jia Zhigang; Chen Xiaobo; "Trusted Communication System Based on RSA Authentication," Education Technology and Computer Science (ETCS), 2010 Second International Workshop on , vol.1, no.,Pp.329-332, 6-7 March 2010.

[11] Ali, A.; Aliyar, L.; Nisha, V.K.; , "RC5 encryption using key derived from fingerprint image," Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference , pp.1-4, 28-29 Dec. 2010.

[12]. Suresha ,Nalini N” Evaluation of Performance of Ciphers for Routing Protocols in Distributed Sensor Networks” International Journal of Data & Network Security, Oct, 2012

[13] C. Karlof and D. Wagner. Secure routing in wireless sensor networks: Attacks and countermeasures. Elsevier’s AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 1(2–3):293–315, 2003. Also appeared in 1st IEEE International Workshop on Sensor Network Protocols and Applications.

[14]. PekkaRiikonen:http://iki.fi/priikone/docs/rsa.pdf 29.9.2002

[15] Abdo Saif Mohammed, M.N.Shanmukh aswamy "A Novel Algorithm to Select Cluster Heads with Highest and Balanced Energy in Wireless Sensor Networks” International Journal of Computer Applications (0975 –8887) Volume 54– No.4, September 2012

AUTHORS

Mr.Abdo Saif Mohammed Completed his B.Sc.degree in Computer Science & Information Systemfrom University of Technology-IRAQ in the year 2001, M.Sc. in Computer Communication fromBharathiar University-India in the year 2009. And He is presently working in the Department of Computer Science, Thamar University Yemen, Dhamar, Yemen. He is doing his Ph. D in the area ofWireless sensor networks under the guidance of Dr.M.N Shanmukhaswamy.

Dr.M.N.Shanmukha Swamy completed his B.E. degree in Electronics and Communication from Mysore University in the year 1978, M.Tech in Industrial Electronics from the same university in the year 1987 and obtained his PhD in the field of Composite materials from Indian Institute of Science, Bangalore in 1997. He is presently working as Professor in the Department of Electronics andcommunication, Sri Jayachamarajendra college ofEngineering, Mysore, Karnataka, India. He is guiding several research scholars and has published many books & papers both in National & International conferences & journals. His research area includes Wireless Sensor Networks, Biometrics, VLSI and composite materials for application in electronics.