Energy Efficient and Secure Routing Protocol for Wireless Sensor Network

V. Vasanthi[1] V. Vinuraja[2] Christopher[3]
[1]P.G Scholar [2]Assistant Professor [3]Design Engineer
[1,2,3]Department of Electronics & Communication Engineering
[1,2]Sri Eshwar College of Engineering Coimbatore, India [3]Caliber Interconnect Solutions, Coimbatore, India

Abstract— Wireless Sensor networks (WSNs) are vastly scattered networks of tiny, trivial wireless nodes, deployed in large counts to scrutinize the milieu or system by the measurement of physical parameters such as temperature, pressure, or relative humidity. For these necessities of WSNs, high efficient routing protocols design ought to energy efficient as feasible to extend their lifetime, and secure data delivery. And designed protocol must be adaptable for sensor nodes mobility which may be static or dynamic. For these needs an energy-balanced routing method based on uniform distribution of energy is designed with change of cluster head for each round of data transmission. This energy efficient algorithm is proposed with verification algorithm which ensures that the secure data transmission is achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors. Cluster based wireless sensor networks maximize the node lifetime and these clusters are formed periodically and dynamically. We propose Short path Secure and Efficient data Transmission protocols for sensor networks where security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is essential for WSNs, while its security relies on the hardness of the discrete logarithm problem. The calculations and simulations are provided to exemplify the competence of the proposed protocols. The results show that, the anticipated protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

Key words: Uniform Energy Distribution, Secure Aggregation, Node Mobility, Wireless Sensor Networks

I. INTRODUCTION

Holocene industrial debuts made in electronics and wireless communications have fostered the enlargement of WSNs [1], [2]. A WSN is a self-organization wireless network system normally dwells of many small, low cost, low-power communication devices called sensor nodes. Each sensor node has limited on-board processing, inadequate storage and radio capabilities [3]. Owing to the limited communication ability and Non-rechargeable energy supply (e.g. battery), WSNs have rigorous requirements about power consumption. Therefore energy-efficient protocols are vital to save energy and protract network lifetime [4]. Micro sensors are deployed to monitor the sensing field and collect information from physical or environmental condition and to co-operatively pass the collected data through the network to a main location. Traditionally there are two approaches to accomplish the data collection task: Single-hop and Multi-hop forwarding. In single hop wireless communication (Direct), the sensor nodes upload data directly to the sink, which may result in long communication distances and degrade the energy efficiency of sensor nodes. But in multi-hop forwarding, data are transferred from the nodes to the sink through multiple relays, and thus communication distance is reduced. However, since nodes closer to the sink have a much heavier forwarding load, their energy may be exhausted quickly, which degrades the network performance [4] – [6].

Clustering is an effective technique to reduce energy consumption in WSNs. In clustering algorithm, a number of nodes in a network will be chosen as the cluster heads (CHs) and the remaining nodes will be regarded as the cluster members (CMs). CMs will form connections with the CHs. A head node will collect data from its CMs and the actual data transmitted to the base station (BS). In WSN clustered hierarchical routing protocols, at times CMs are closer to the sink than CH, but it should transmit data to CH earliest. This backward transmission result in waste of energy.

In paper [10] a new energy-balanced routing protocol is used which uses forward transmission area (FTA) based on position of sink and final data flow direction to avoid backward transmission [6]. Nevertheless, most of the existing in-network data aggregation algorithms have no provisions for security. A compromised node might endeavor to ruin the aggregation process by induction several attacks, such as eavesdropping, congestion, message sinking, message invention, and so on [8]. This paper focuses on one of the most troublesome attacks: the falsified sub aggregate assail, in which a compromised node relays a false sub aggregate to the parent node with the aim of injecting error to the concluding value of the aggregate computed at the base station.

II. RELATED WORK

A. Low Energy Adaptive Clustering Hierarchy (Leach) Protocol:

In LEACH, all the nodes in a network organize themselves into local clusters. The protocol is divided into a setup phase when the clusters are organized and a steady state phase when CH receive data from all the CMs, perform data aggregation and transmit data to the remote base station.

The operation of LEACH in time slots is illustrated in Fig1. In the steady-state phase, operation is broken into frames where nodes transmit their data to the CH at most once per frame during their allocated transmission slot. To reduce energy dissipation, each CM sets the amount of transmission power by using power control. It is based on the received strength of the cluster-head advertisement.

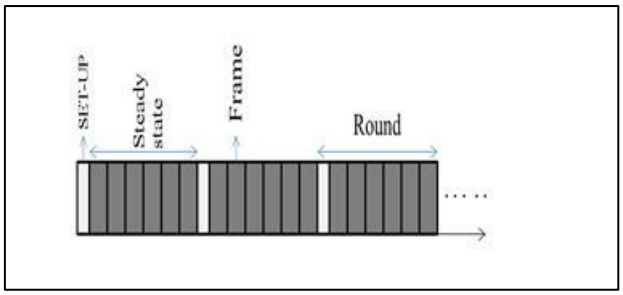
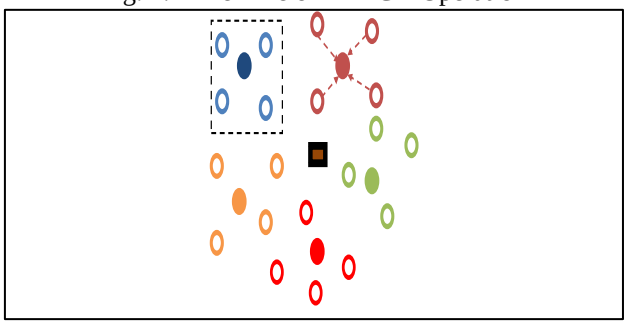


Fig. 1: Time Line of LEACH Operation



Base station
Data from nodes to CH
Data from CH to Base station

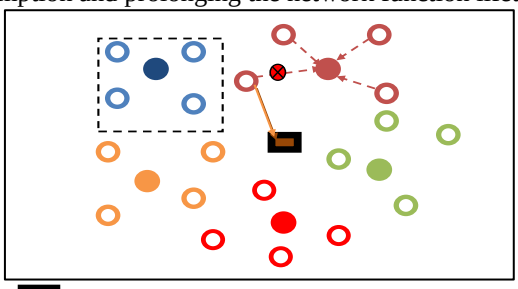
Fig. 2: Data Transmission

The CH receives all the data from the nodes in the cluster by keeping its receiver on and then the resultant data are sent from the CH to the base station. In clustering algorithm, CH node is much more energy-intensive than a CM. Thus, when a CH node in a cluster dies, all the CMs inside that cluster drop communication ability.

B. Forward Aware Factor - Energy Balanced Routing Method (FAF-EBRM):

In WSN routing protocol, sometimes cluster members in a cluster are nearer to the sink than the Cluster Head, but it should transmit data to CH foremost. It results rearward transmission of data and thus leads to devastate of energy. This trustworthy path method results in reduced energy consumption and this routing model is shown in Figure.3.

In this method, an energy-balanced routing protocol is designed that uses forward transmission area (FTA) based on position of sink and final data flow direction. In other words, FTA define forward energy density which constitutes forward-aware factor with link weight, and propose a new communication protocol based on forward-aware factor, thus balancing the energy consumption and prolonging the network function lifetime.



Base station
Data from nodes to CH
Data from CH to Base station
Direct transmission (from node to CH)

Fig. 3: FAF-EBRM Reliable Path

III. SECURE AGGREGATION OF MOBILE NODES

A. Network Model:

The Sensor nodes are haphazardly distributed in a W x H rectangular sensing field. Data are sent to the regional central node and then transferred to the sink node. The simulation results are shows in a Network AniMation (NAM) window of Network Simulator 2 (NS2).

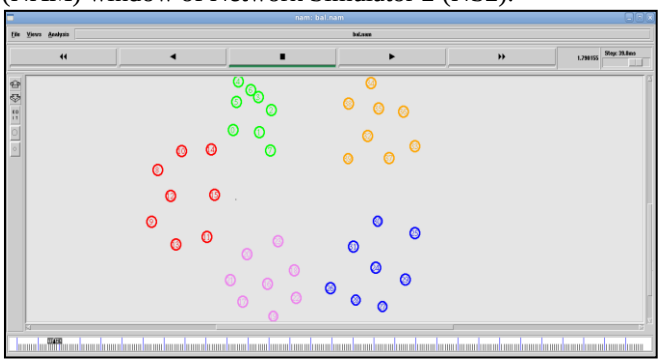


Fig. 4: Sensor Nodes Deployment and Nodes Are Grouped By Cluster

In Fig.4 sensor nodes are deployed in the environment and nearby nodes are form a group which is known as Cluster. In the NAM window each cluster is differentiated by colors.

The descriptions of the model as follows,

- All sensor nodes are isomorphic and they have limited energy to compute, communicate and data storage.
- Sensor nodes are deployed unattended environment, so energy is limited.
- While the sensor nodes are tiny, the memory size is also limited.
- Nodes can vary transmission power according to the distance to the sink node.

B. Uniform Energy Distribution:

The election procedure is as follows.

- The node broadcasts energy request message (ENE_REQ) along with its individual energy level information to the remaining nodes inside cluster.
- The left over nodes its energy level with the nearest elector nodes energy level.
- Then energy reply message (ENE_REP) is send by remaining nodes if any of its energy level is higher than elector nodes energy level, else it hold off for cluster head advertisement message (CH_ADV).
- If energy of elector node is greater than remaining nodes energy level then it becomes cluster head otherwise elector node selects the node with maximum residual energy as the cluster head and successive maximum residual energy as the next elector node.
- The Cluster head selection procedure is repeated for each round of operation that is after each round of data transmission.

1) Algorithm 1 Cluster Head Selection Phase:

Cluster ← nil;

Round ← 0;

Better signal ←0;

Set_number ←{};

Last Round CHi ←-1/P;
Advertisement.timeout()
begin
Round i ← Round i +1
if Round i – Last Round CHi > 1/P then

$$Ti \leftarrow \frac{P}{1-P*(\text{Round i mod}(\frac{1}{P}))};$$

else
Ti ← 0;
end if;
rand i ← uniform (0,1);
if rand i < Ti then
cluster i < i;
Last Round CHi ←Round i;
Set Member i ← {};
Send ADVi to all nj € N;
else
Better signal I ← 0;
end if;
Receive (msg i such that origin i(msg i) =(ni,nj))
begin
if msg I =ADVj and signali(msgi) > Better signal i then
Better signal i ← Signali(msgi);
Cluster I ← j;
End if;
if msgi = MEMBERj(i) and cluster i = i then
set Member I ← set member i U nj;
end if;
end;
confirmation.timeout()
begin
if Cluster i ≠ i then
send MEMBERi(cluster i) to all nj € N;
end if;
end;

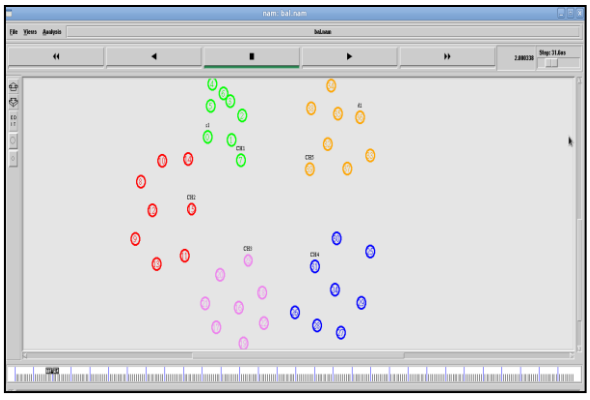


Fig. 5: Cluster Head Selection for Each Group of Nodes

As shown in Fig.5. Energy efficient algorithm picks out the higher residual energy node to pretend as a cluster head node. For next round of transmission, again higher residual energy node is selected as cluster head.

C. Data Transmission Phase:

Once the cluster is formed diffusion of data takes place. Inside the cluster only nodes located in multicast path are in awaken state and only those nodes are involved in data transmission progress. Data transmission is started from the source node to destination node in the shortest path in the whole network. And this feasible path data transmission is shown in Fig.5.

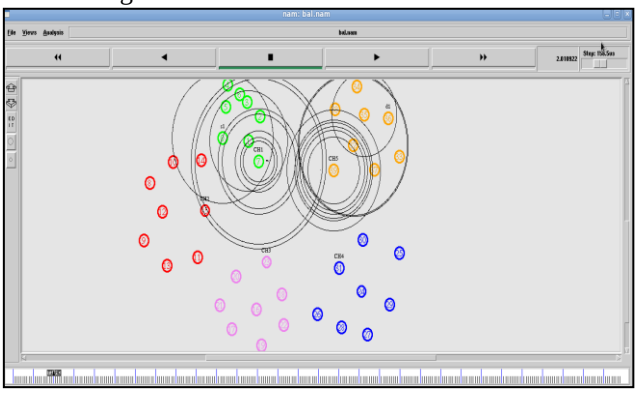


Fig. 6: Data Transmission from One Cluster to Another in Feasible Path

The implementation of this technique also results in reducing the attenuation level of snooping. Also algorithm facilitates for the reception of new node from other clusters when the current cluster is in demand for ordinary sensor nodes. The transmission of data inside each cluster is based on TDMA technique in which time is divided into periodic cycles. This further reduces the collision level of data transmitted from ordinary sensor nodes.

D. Data Accuracy Phase:

In this paper verification algorithm is utilized along with Energy efficient algorithm in order to get better level of security. Each cluster head inside definite cluster performs data aggregation of encrypted information being transmitted by ordinary nodes of the corresponding cluster. Each sensor nodes while data transmission, encrypt the data and transmit the cipher text to the Cluster Head. Data aggregators on the other hand does not requires the decryption of cipher text, rather it simply fuse the encrypted data and transmit to the Base station directly.

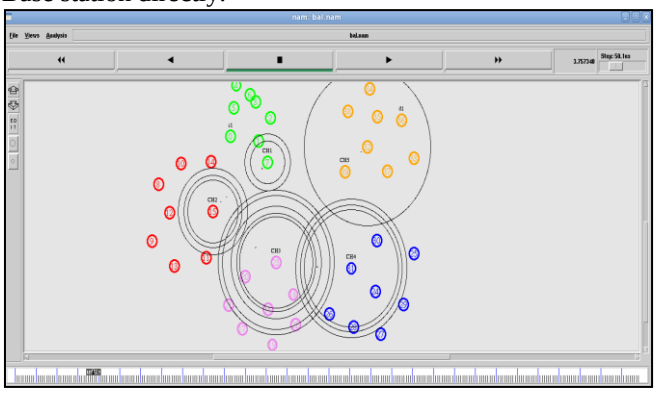


Fig. 7: Secure Transmissions by Transmitting Encrypted Data to the Destination in Different Path

The verification algorithm also used to check the accuracy of data packets being ordained to BS from CH. The secure algorithm is shown in the Fig.7. In a large sensor network, in-network data aggregation significantly reduces the amount of communication and energy consumption. There is a stout aggregation skeleton called synopsis diffusion which combines multipath routing schemes with duplicate-insensitive algorithms to accurately compute

aggregates (e.g., predicate Count, Sum) in spite of significance losses ensuing from node and diffusion failures.

However, this aggregation framework does not address the problem of false sub aggregate values contributed by compromised nodes which results in large errors in the aggregate computed at the root node. This is one of the major problems in sensor networks since these are highly vulnerable to node compromises due to the unattended nature of sensor nodes and the lack of fixed-resistant hardware. The synopsis diffusion approach secure against attacks in which compromised nodes contribute false sub aggregate values. In order to achieve this, a lightweight verification algorithm by which the base station can determine if the computed aggregate includes any false contribution. This minimizes the per-node communication overhead in our algorithm.

1) Algorithm 2 Secured aggregation (R, Wx, K)

1) Begin
2) Receive {(A′x^1, M$^{\times 1}$), (A′x^2, M$^{\times 2}$),……,(A′x^n, M$^{\times n}$)} from ordinary nodes;
3) A′x = W' x| A'x^1| A'x^2| ……. |A'x^n; // cipher text aggregation by cluster head;
4) Pq* = index of qth rightmost "1" bit in A′x, for 1≤ q ≤ k′, where k′is largest integer but lesser than k;
5) A′x possibly will have fewer than k "1" bits where k' < k. // generate a MAC bit for Pq* in Q'x, for 1≤ q ≤ k';
6) Assemble the unification of M of the received MAC's; arbitrarily choose M^x = {MI1*, MI2*,……., MIk* } from M; broadcast (A'x, M*) to parent nodes;
7) End

E. Node Mobilty:

The algorithm also facilitates for the acceptance of new node from other clusters when the current cluster is in demand for ordinary sensor nodes which is shown in Fig.8.

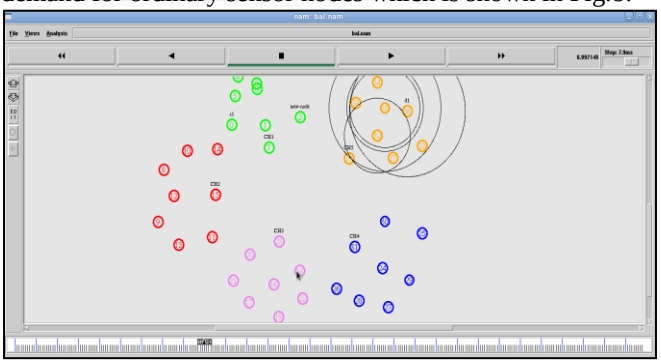


Fig. 8: Node Mobility from Cluster 1 to Cluster 5

F. Short Path Efficient and Secure Transmission Routing:

The scheme implemented for CWSNs consists of the subsequent operations, particularly, system at the BS, key mining and signature signing of the data transfer nodes, and substantiation of the data receiving nodes.

1) System:

The BS (as a trust authority) generates a master key msk and public parameters param for the private key generator (PKG), and gives them to all sensor nodes.

2) Key Mining:

Given an ID string, a sensor node generates a private key sekID associated with the ID using msk.

3) Signature Signing:

Given a message M, time-stamp t and a signing key θ, the sending node generates a signature SIG.

Substantiation: Given the ID, M and SIG, the receiving node outputs "accept" if SIG is valid, and outputs "reject" otherwise.

4) Short Path:

Transfer of key in the shortest path from the source node to destination node.

IV. Simulation Results

In this section, the report investigates the simulation cram that examined energy consumption and accuracy of proposed algorithm. The evaluation result shows the better performance metrics for the parameters such as energy, enhanced lifespan and data security.

A. Simulation Environment:

Simulations were performed by using Network Simulator2 (NS2) environment which is a powerful platform for network research process and it is a discrete event driven simulator tool. In the environment, 50 nodes are randomly deployed in a 300m x 300m area. The performance of our secure energy balanced routing method is evaluated in terms such as the total number of received packets at the BS, network lifetime and the security level of the received packets.

B. Results and Discussion:

In the proposed technique, secure energy balanced algorithm is used for the transmission and aggregation of the data packets which outcomes with condensed energy consumption and hence protracts the networks lifespan. The verification algorithm works together with previous algorithm to check the accuracy of data packets being ordained to BS from CH.

1) Energy Consumption:

In each simulation of experiment, the energy assign to nodes are changed with number of packets. Energy consumption of each cluster head in the simulation network named node1, node7, node32, node37 is shown in Fig.7. The energy usage by the nodes is differing in terms of transmission of data. Comparing some nodes energy node 1 energy consumption is low compared to other nodes.

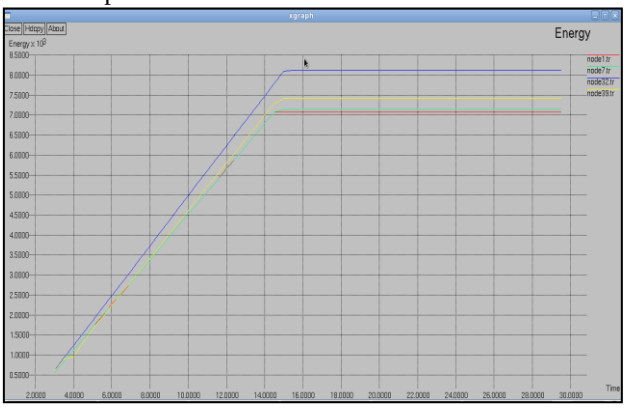


Fig. 9: XGRAPH for Energy Consumption by Nodes

2) Data Accuracy:

The accuracy metric is defined as the ratio between the collected summation by the data aggregation scheme used and the real summation of all individual sensor nodes. Data

accuracy of nodes node1, node35, node36 is shown in Fig.8. Accuracy level of node 36 is high compared to other nodes accuracy level.

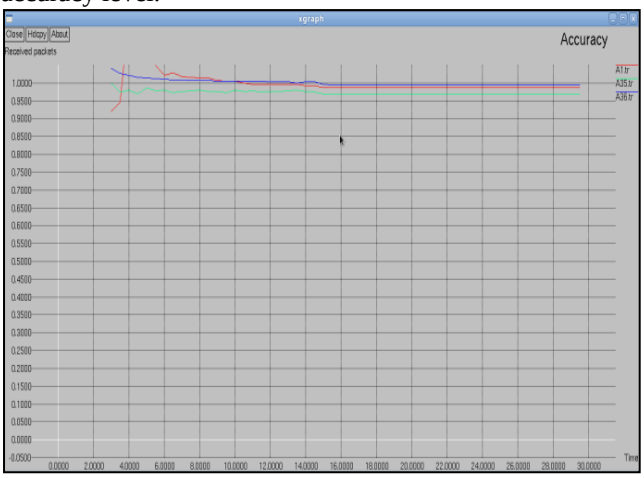


Fig. 10: XGRAPH for Accuracy of Individual Nodes

V. CONCLUSION

In Wireless Sensor Networks, battery life and the resource discretion plays a vital role. Secure Energy Balanced Routing Method based for WSN is proposed to improve multiple metrics. This algorithm provides secure data diffusion, energy efficient by changing the role of cluster head. The main spotlight of this technique is to optimize the recital metrics such as network lifespan, energy consumption and data security. By applying sleep scheduling method and reducing the efforts of the working nodes energy efficiency can be made superior. The aggregation of data packets results in compacted data packets which further reduces the transmission trouble and also provides extent for security and source coding. Thus the sensor data's are associated and transmitted with higher-ranking efficiency which comes as a result of cryptographic and data compression techniques. Short path Secure and Efficient Transmission routing is efficient in communication and applying the Identity based crypto system, which provides security requirements in CWSNs.

REFERENCES

[1] Degan Zhang, Guang Li, Ke Zheng, Xuechao Ming and Zhao-Hua Pan, "An Energy-Balanced Routing Method Based on Forward-Aware Factor for Wireless Sensor Networks," IEEE Trans. on Industrial informatics, Vol. 10, pp. 1, February 2014.

[2] Huang Lu, Jie Li and Mohsen Guizani, " Secure and Efficient data transmission for Cluster-based wireless sensor network", IEEE Transactions on parallel and distributed systems, Vol. 25, pp. 750-761, March 2014.

[3] A. L. Barabasi, "Scale-free networks: A decade and beyond," Science, vol. 325, no. 5939, pp. 412–413, 2009.

[4] D. G. Zhang and X. D. Zhang, "Design and implementation of embedded un-interruptible power supply system (EUPSS) for web-based mobile application," Enterprise Inf. Syst., vol. 6, pp. 473–489, 2012.

[5] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application- specific protocol architecture for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 1, pp. 660–670, Oct. 2002.

[6] I. K. Samaras and G. D. Hassapis, "A modified DPWS protocol stack for 6LoWPAN-based wireless sensor networks," IEEE Trans. Ind. Inf., vol. 9, no. 1, pp. 209–217, Feb. 2013.

[7] D.G. Zhang, "A new approach and system for attentive mobile learning based on seamless migration," Appl. Intell., vol. 36, no. 1, pp. 75–89, 2012.

[8] J. Aweya, "Technique for differential timing transfer over packet networks," IEEE Trans. Ind. Inf., vol. 9, pp. 325–336, Feb. 2013.

[9] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[10] Q. J. Chen, S. S. Kanhere, and M. Hassan, "Analysis of per-node traffic load in multi-hop wireless sensor networks," IEEE Trans. Wireless Comm., vol. 8, pp. 958–967, Apr. 2009.

[11] Jiong Jin, Avinash Sridharan, Bhaskar Krishnamachari and Marimuthu Palaniswami, "Handling inelastic traffic in wireless sensor networks," IEEE Trans. Sel. Areas Commun., vol. 28, pp. 1105–1115, Jul. 2010.

[12] D. G. Zhang and X. J. Kang, "A novel image de-noising method based on spherical coordinates system," EURASIP J. Adv. Signal Process., vol. 1, pp. 110, 2012.

