A Novel Approach to Balance the Trade-Off between Security and Energy Consumption in WSN

K Jaya Shankar Reddy
Dept of Computer Science and Engineering
National Institute of Technology
Andhra Pradesh
Email: kommurujaishankarreddy@gmail.com

K Karthikeya Yadav
Dept of Computer Science and Engineering
National Institute of Technology
Andhra Pradesh
Email: abhikaradi@gmail.com

BKSP Kumar Raju Alluri
Dept of Computer Science and Engineering
National Institute of Technology
Andhra Pradesh
Email: pavan0712@gmail.com

***Abstract*—WSN (Wireless sensor networks) consist of a huge number of non-rechargeable tiny sensor nodes deployed in an environment which sense the data and transmit to the base station. A sensor becomes useless once its energy is exhausted thereby reducing the overall lifetime of the network. Also, WSN find their use in data confidential applications like military communication system and encryption is vital in such cases. However, there is always a trade-off between improving security and reducing energy consumption. There are various algorithms which provide security but most of them are complexity bound. As the complexity of security algorithm increases, the energy consumption increases. To balance the trade-off, we came up with a novel approach, which uses low complexity XOR technique and Hybrid LEACH-PSO algorithm. Through extensive simulations, it is identified that the proposed approach performs better than the existing approaches.**

***Keywords*—** Wireless Sensor Networks, Cluster Head, Cryptography, Security, Particle Swarm Optimization, LEACH, Base Station, Routing, Energy.

I. Introduction

WSN (Wireless Sensor Networks) are the networks formed by a huge number of sensor nodes which have data storing and data transmitting capabilities [1]. These sensor nodes are randomly deployed in an environment to sense the physical parameters in and around their vicinity. The sensed data needs to be communicated to the base station or sink and then transmitted to a server for further investigation of the environment. Since the nodes have to transmit the sensed data, each time they need a fixed amount of energy for transmission. The energy consumption needs to be taken care as the nodes are non-rechargeable. The communication is established either through single-hop or multi-hop with the help of a routing protocol in the WSN.

The presence of intruder or attacker in the route between the node and the base station may lead to data breach. To overcome this, the data needs to be encrypted before transmitting the data from the sensor node. Famous security algorithms like AES and RSA have been used in the literature [2] to encrypt the data. However, because of their complexity, the nodes use more energy for encrypting rather than using for their main responsibility, i.e. transmitting. This reduces the lifetime of the network and the number of packets sent to the base station. Also, this causes an increase in the number of dead nodes with respect to time which is not the goal to be achieved using WSN.

To overcome this problem, a less complex XOR technique has been used for encryption [3]. Redundancy of operations is identified as a setback to this technique. In this paper, we propose a non redundant XOR approach and it provides better security than that of the redundant one.

Not only for the transmission of the data, the encryption of data also requires energy from the sensor nodes. Irrespective of the encryption algorithm used for transmitting the sensed data, there is a need to reduce the overall energy consumption of the sensor nodes in the network.

To reduce the energy consumption, the famous LEACH (Low Energy Adaptive Clustering Hierarchy) protocol [4] and the Bio-Inspired PSO (Particle Swarm Optimization) algorithm [5] are being used for generating less energy consuming paths from the sensor node to base station. Taking the advantages of the above two methods into consideration, we propose a new routing algorithm named ”Hybrid LEACH-PSO” which performs better than that of using the two algorithms individually.

A. Problem Statement

Our approach aims to balance the trade off between the energy consumption and security improvisation in WSN.

B. Proposed Approach

To satisfy the data confidentiality, we propose a new and non redundant XOR technique. To reduce the energy consumption in terms of generating optimized routes or paths, a novel approach that uses hybrid LEACH- PSO algorithm is proposed.

The rest of the paper is organised as follows. Section II deals with related work. Section III discusses the proposed non-redundant XOR technique. Section IV describes the novel approach for improving the life span of WSN nodes. Section V discusses the simulation results proving that the proposed approach a better one. Finally, the conclusion is discussed in Section VI.

II. RELATED WORK

WSN find its applications in various fields like military, forests and homeland. The WSN have many mission-critical tasks. Security is crucial in such networks. Providing security in WSN is difficult due to the resource limitations of WSN. There is always a conflict between resource consumption and security maximization. Overall cost of WSN should be as low as possible and also security must not be compromised. To achieve that we came up with an approach named non-redundant XOR technique. A Symmetric and an Asymmetric algorithm have been used for the comparison purposes. AES is the most popular Symmetric and RSA is the most popular Asymmetric algorithm. The following section describe each algorithm briefly.

A. AES

AES (Advances Encryption System) is an Iterative Cipher. It is based on substitution - permutation network. AES represents the text in terms of bytes rather than bits [6]. It is used for the encryption of 128 bits (12 bytes) , 192 bits (14 bytes) and 256 bits (32 bytes).

AES uses 10 rounds for 12 byte keys, 12 for 14 byte keys and 14 for 32 byte keys. The encryption and decryption are exactly reverse of each other. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built in future-proofing against progress in the ability of perform exhaustive key searches. However, the AES security is ensured only if the symmetric key management is done properly.

B. RSA

RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. Since it is an Asymmetric cryptographic algorithm, it has two keys, private key and public key. Here the public key will be shared with the base station and the private key should be kept with the sensor node itself. This Algorithm represents the text in terms of bits [7].

1) Encryption Function: It is the function used for converting the plain text into the cipher text and it can be reversed only with the knowledge of private key.

2) Key Generation Function: The difficulty of cracking the private key from a RSA public key is equivalent to factoring the product of two large prime numbers. An attacker cannot crack the private key unless the factoring is done. It is also a one way function, going from products to the number, but from number to factors is difficult.

As, the key length increases, the security increases and becomes difficult for the attacker to crack the private key. The sensor node encrypts the data before transmitting to the next hop. Once encrypted and transmitted, the decryption takes place at the Base Station.

C. Redundant XOR technique

This technique uses asymmetric key cryptography. The cryptography technique that is chosen for WSNs has to be appropriate such that they meet the limitations or constraints of WSN like energy consumption, memory and lifetime of the WSN. Thus we use simple XOR technique to reduce the complexity of algorithm so that we can minimize energy consumption of WSN.

Encryption of data takes place at WSN where as decryption is done at base station. Each node is assigned with a unique number from 1 to N (number of nodes). There will be two keys used in this technique. One key is dynamic i.e. it is generated for each node in every round, so the intruder will not be able to guess the key as it is not constant and second key is a static key which is assigned to every node and it will be constant in every round.

First, data at each node is encrypted with the dynamic key by performing XOR operation on data with the dynamic key. Then encrypted data is again encrypted with the corresponding fixed key, the final encrypted data is sent to the base station where decryption takes place. The algorithm has two variations:

In the first case, the number of encryptions at k^{th} node is equal to k times where k is any integer between 1 and N. So in this case, number of encryptions that takes place in the network is dependent on the number of nodes. Let say, at 2^{nd} node encryption takes place two times, at 3^{rd} node encryption takes place 3 times, 4^{th} node four times, 10^{th} node ten times and so on till N times at N^{th} node. In the improved model number of encryptions that takes place at each node in the network varies randomly between:

i. [1 and N/2]

ii. [1 and N/4]

The number of encryptions and decryptions that takes place here is less as compared to the first one and 2^{nd} case is more efficient than the previous one in terms of memory and energy consumption. Also in terms of security the later one is better than the former as encryption and decryption takes place randomly so it becomes difficult for the attacker to hack the data. So the algorithm consists of only two keys for each node in which static key is known to base station, so that we need not send the key to base station where as we have to send dynamic key to the base station as it changes in every round. The double encryption algorithm comprises of only two keys at each node in the sensor network and it is a low storage cryptographic technique.

III. Proposed Non Redundant XOR technique

A. Drawback in Redundant XOR technique

In this technique we first encrypt the data with dynamic key once and then we encrypt the encrypted data with static key k times where k in first case is node number. In the second case, encrypted data is encrypted with a static key k times where k is a random number generated between 1 and N/2 (N/4). In both the cases we are encrypting the encrypted data repeatedly with the same static key. Performing XOR operation on some data D repeatedly with same key even number of times will yield to D itself. Similarly performing XOR operation odd number of times would yield to D^1 where D^1 is equivalent to performing XOR operation only once.

To overcome the drawback we came up with an algorithm named non redundant XOR technique.

In the proposed algorithm, we first encrypt the message with the static key. Then encrypt the encrypted data with the dynamic key k times where k is the node number. The proposed approach varies with the existing XOR redundant technique in terns of frequency of key change i.e. each iteration of k iterations dynamic key is changed so that we can get different encrypted data in each iteration (Equation 1).

$$DynamicKey = (DynamicKey + k) mod(2^m - 1) \qquad (1)$$

where,

m is number of bits in key

k is node number

Thus we are removing the redundancy from the above algorithm so that we can get different encrypted messages in each round. The complete algorithm is explained in Fig. 1.

Two variants of the non redundant XOR techniques are proposed to make the network more secure.

1) Dynamic Key Position Placement: Here position of dynamic key is P where P is generated randomly between two and length of the message and key is kept in that position. This position P is kept at the starting of the message. Base station checks start of the message, retrieves P from the message, goes to the position P to extract the dynamic key and hence decrypt the encrypted data.

2) Encrypting Dynamic Key: Dynamic key is encrypted with a new key which is generated randomly. This encrypted dynamic key is sent with data along with the second dynamic key which is used to encrypt the dynamic key. The positions of encrypted dynamic key and second dynamic key can be static which is known to base station or the positions can be changed dynamically using dynamic key position placement method.

IV. IMPROVING THE LIFE TIME OF WSN

A. motivation

The energy of the each sensor node is used for encrypting the data and transmitting the encrypted data. So, a part of the node's energy is utilized for encrypting and there is a need to reduce the energy consumption. For this a novel Hybrid LEACH PSO based routing algorithm is proposed which performs better than the individual algorithms.

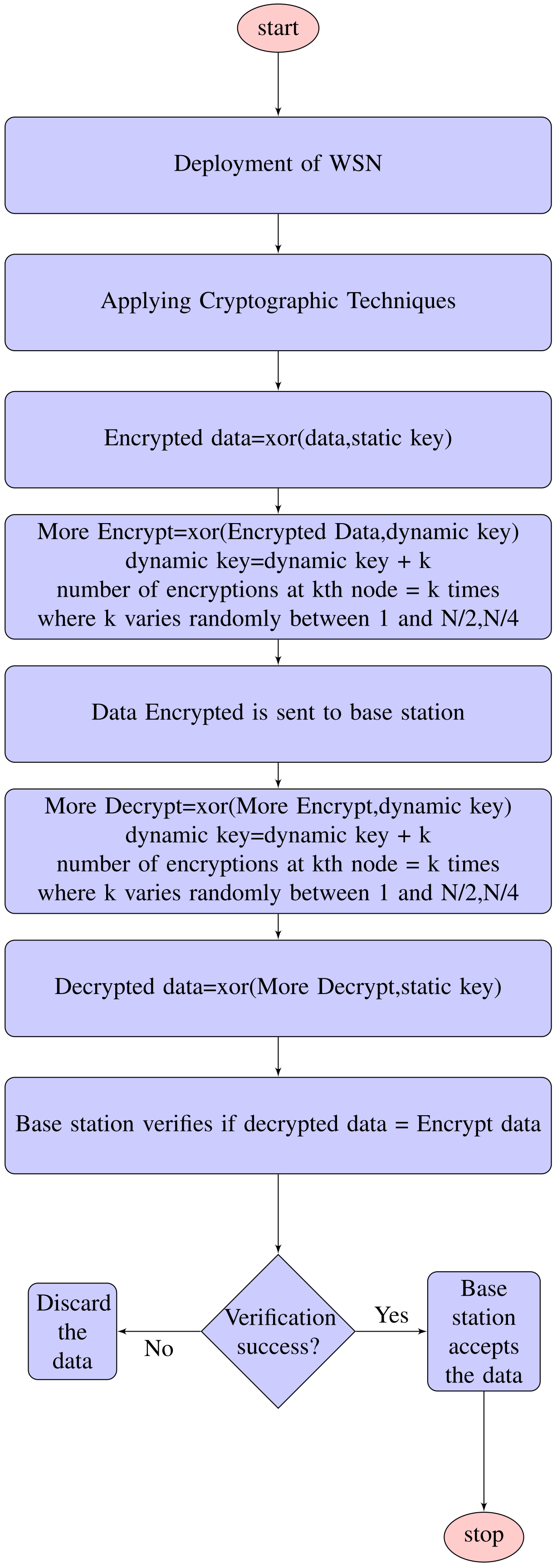
start
Deployment of WSN
Applying Cryptographic Techniques
Encrypted data=xor(data,static key)
More Encrypt=xor(Encrypted Data,dynamic key)
dynamic key=dynamic key + k
number of encryptions at kth node = k times
where k varies randomly between 1 and N/2,N/4
Data Encrypted is sent to base station
More Decrypt=xor(More Encrypt,dynamic key)
dynamic key=dynamic key + k
number of encryptions at kth node = k times
where k varies randomly between 1 and N/2,N/4
Decrypted data=xor(More Decrypt,static key)
Base station verifies if decrypted data = Encrypt data
Discard the data
No
Verification success?
Yes
Base station accepts the data
stop

Fig. 1. Proposed Non Redundant XOR technique

B. LEACH

LEACH (Low Energy Adaptive Clustering Hierarchy) protocol is the oldest protocol among the hierarchy protocols and it is of milestone significance in WSN. The main aim of the LEACH protocol is to minimize the energy consumption. This is done by electing cluster heads among the sensor nodes, and whenever a sensor node senses the data and sends data to its closest reachable cluster head. Cluster head's responsibility is to transmit data to the Base Station. This process is divided into the following phases.

1) Setup Phase: In this phase, the cluster heads are elected by a stochastic probability algorithm. Each node uses a stochastic algorithm at each round whether it is to become a cluster head or not. Nodes that are currently the cluster heads cannot be the cluster heads for the next P rounds. Here P is the desired percentage of the cluster heads to be selected in each round. So, 1/P is the probability of sensor node to be selected again as a cluster head.

2) Steady phase: In this phase, each cluster head advertises its availability to the other surrounding sensor nodes. Each sensor nodes gets associated with one of the cluster heads using the RSS (Received Signal Strength). It is important to note that the RSS is directly proportional to the distance in an optimistic environment.

In each round, each cluster head initiates a time-division multiple access schedule for each of the sensor nodes allocated to it. Each sensor sends its corresponding data, if available, to the cluster head. The cluster head then aggregates the data and transmits the aggregated data to the Base Station.

LEACH protocol balances the energy consumption among the network nodes because of its periodic and random selection of cluster heads. But the disadvantage of LEACH is that, there are no hops used for transmission of the aggregated data from the sensor node to the base station. Because of this, the selected cluster head energy can be depleted quickly as the distance between the cluster head and base station is more.

C. Particle Swarm Optimisation (PSO)

Particle Swarm Optimisation [8] is a nature inspired algorithm from the migration of flock of birds. It is a population based stochastic technique developed by Kennedy and Eberhart (1995). It optimizes a function known as Objective Function for which a swarm (group) of particles acts as input. The PSO algorithm requires random initial population of feasible inputs for the objective function. This is called as initialization phase. Iterations are performed updating the velocities and positions of the particles, and at each iteration tracking each particle's best solution and the global best among all particles best solutions (Equations 2 and 3). This is called the update phase. At the end of the iterations, the particle which gives the global best is the possible input for which the objective function is maximized or minimized.

Velocity Update:

$$V_i = w \times V_i + C_1 \times r_1 \times \big(P_i - X_i\big) + C_2 \times r_2 \times \big(G_i - X_i\big) \tag{2}$$

Position Update:

$$P_i = P_i + V_i \tag{3}$$

where,

i is the id of the particle in the population.
V_i is the velocity of i^{th} particle.
P_i is the best position of i^{th} particle.
G_i is the Global best of i^{th} particle.
X_i is the position of i^{th} particle.
C_1 is the coefficient of social-component.
C_2 is the coefficient of self-component.
w is the coefficient of inertial weight.
r_1, r_2 are random numbers between 0 and 1.

PSO algorithm is used in WSN to reduce the energy consumption or improve the life time of the network. This is done by selecting the multi-hopped shortest path from the sensed node to the base station. A path from the sensor node to the base station can be represented as a chain of sensor nodes ending with the BS.

In the initialization phase of PSO, it generates all the feasible set of nodes, i.e. paths from sensor to the BS. Each particle is represented as a priority queue so that the node which is having the next high priority is chosen as the next hop. In this way, it reaches the BS.

In the update phase, new paths are generated as the priority queue of each particle is updated in each iteration. Each path generated is given as input to the objective function (Equation (4)) and the corresponding costs are calculated.

$$a = w_d \times D + w_r \times E.R + w_s \times S.E \tag{4}$$

where,

$\mathrm{w_d}$ is the weight associated with distance of the path.

D is the total distance of the path.

$\mathrm{w_r}$ is the weight associated with energy ratio.

E.R is the energy ratio of the path.

$\mathrm{w_s}$ is the weight associated with energy.

S.E is the sum of energies of the hops in the path.

High priority is given to the distance, as more is the distance that is to be transmitted by a node, the more energy is required [9].

Also, the hops between the sensor nodes and the base station should be chosen such that energy of sensor should be as high as possible.

Apart from distance and energy, number of hops between the sensor and base station that are to be active for the transmission of the data should be less. This is given the least priority. Simulations have been run in MATLAB and the PSO based routing protocol has given better results than the LEACH based routing protocol.

D. *Proposed HYBRID LEACH-PSO based Protocol*

The disadvantage of LEACH is that it depletes the selected cluster head to large extent and owing to the PSOs better results than the LEACH, a novel approach has been proposed, i.e. Hybrid LEACH PSO.

In this approach, the cluster head selection is done by the LEACH protocol and then the optimal routing path is generated by the PSO based routing algorithm that connects the selected cluster heads to the BS. So, the cluster head is not going to transmit directly to the base station but using other cluster heads as hops.The parameters of the Hybrid LEACH PSO remain as same as that of the individual protocols. The Objective function is also the same one. The algorithm is explained in Fig. 2.

We observed that the results obtained were much better than that of the LEACH and PSO based routing protocol.

V. EXPERIMENTS AND RESULTS

The network architecture considered has sensor nodes located at random positions and a base station located at center of the environment. Extensive simulations are conducted in MATLAB using the same network architecture. The parameters of the network architecture implemented are shown in Table I.

A. *Security Simulations*

The AES, RSA, redundant and the proposed non redundant XOR algorithms are implemented. The time elapsed for the algorithms with a block size of 128 bits and key size of 128 bits are shown in Table II.

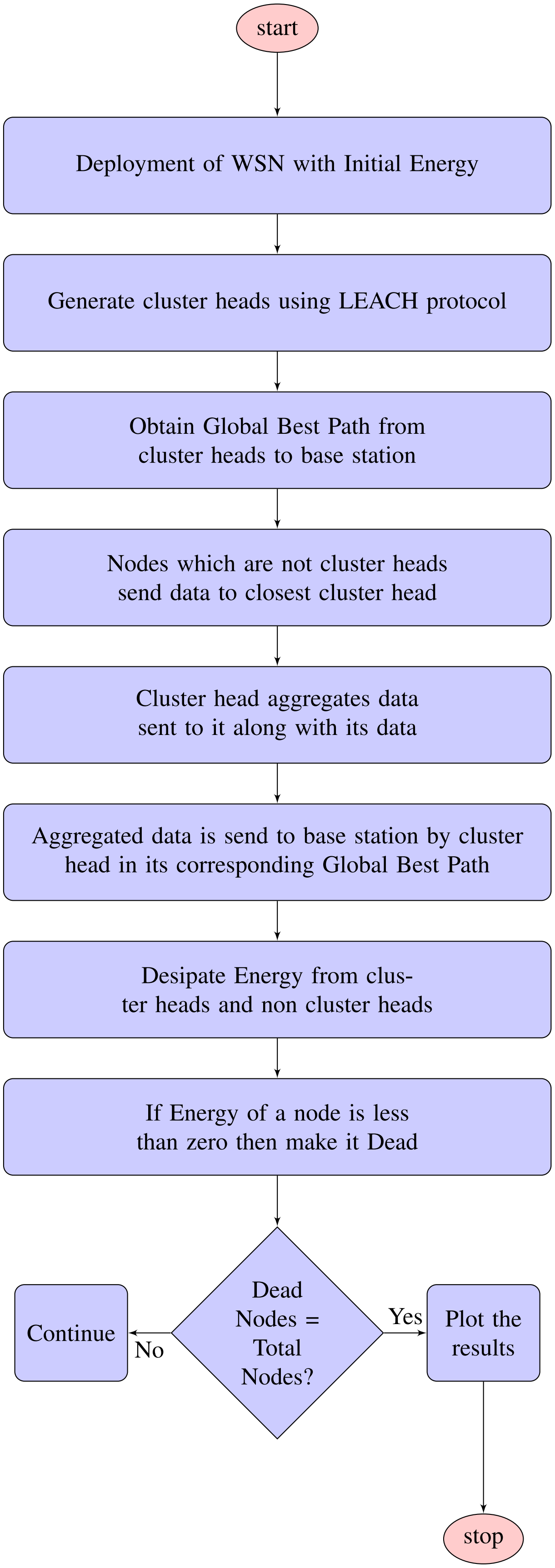
start
Deployment of WSN with Initial Energy
Generate cluster heads using LEACH protocol
Obtain Global Best Path from cluster heads to base station
Nodes which are not cluster heads send data to closest cluster head
Cluster head aggregates data sent to it along with its data
Aggregated data is send to base station by cluster head in its corresponding Global Best Path
Desipate Energy from cluster heads and non cluster heads
If Energy of a node is less than zero then make it Dead
Dead Nodes = Total Nodes?
No
Continue
Yes
Plot the results
stop

Fig. 2. Proposed Hybrid LEACH-PSO algorithm

TABLE I
COMPARISON OF SECURITY ALGORITHMS

Parameter	Value
Initial Energy of the sensor nodes	0.0055 J
Energy depleted to transfer a bit	50*0.000000001 J
Energy depleted to receive a bit	50*0.000000001 J
Free Space Energy	10*0.000000000001 J
Packet Length	200 Bits
Number of iterations in PSO	50
Initial Population	50
Initial Damping Factor	0.98
Personal and Global Learning Coefficient	1.5
Probability p of cluster head	0.1
Aggregation Energy at Cluster Head	5*0.000000001 J

TABLE II
COMPARISON OF SECURITY ALGORITHMS

Algorithm	Time Elapsed
AES	0.024297
RSA	0.110243
Redundant XOR	0.010193
Non Redundant XOR	0.010896

B. Energy Simulations

Three measures, i.e number of dead nodes per round, total energy per round and number of packets sent to the base station are used for the comparing the routing algorithms. The results are shown in Table III.

TABLE III
COMPARISON OF ROUTING ALGORITHMS

Nodes	Algorithm	Packets	Dead Nodes	Total Energy
125	LEACH	1579	123	0.0114
	PSO	2232	123	0.0121
	HYBRID	3253	60	0.1428
250	LEACH	2780	249	0.0033
	PSO	2496	250	0
	HYBRID	5992	187	0.0773
500	LEACH	4874	499	0.0011
	PSO	3126	500	0
	HYBRID	6919	480	0.0191

Simulations are performed for different architectures having 50, 100, 125, 250 and 500 sensor nodes and observed that for each and every architecture hybrid LEACH-PSO has performed better than LEACH and PSO. As number of nodes increases disadvantages of LEACH and PSO would pile up resulting in sending less number of packets to the base station than hybrid LEACH-PSO.

Figures 3, 4 and 5 are obtained by simulating the network with 50 nodes and the results prove that our proposed Hybrid LEACH-PSO performed better than LEACH and PSO individually.

Similarly, Figures 6, 7 and 8 are obtained by simulating the network with 100 nodes and the results prove that our proposed Hybrid LEACH-PSO performed better than LEACH and PSO.

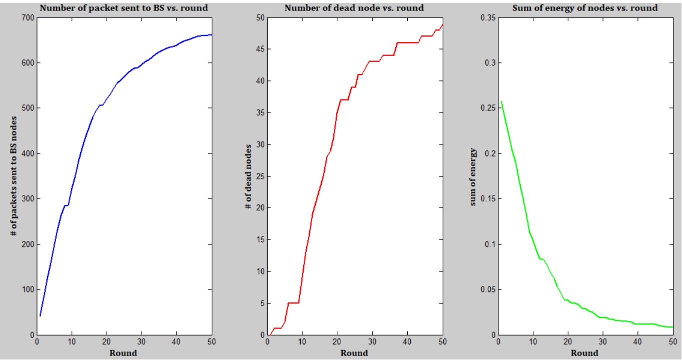

Fig. 3. LEACH results when number of nodes is 50

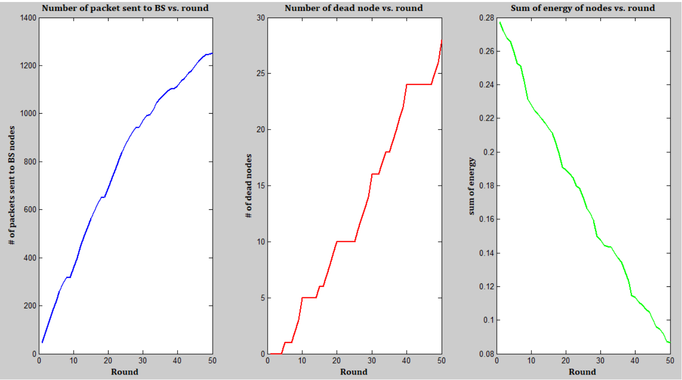

Fig. 4. PSO results when number of nodes is 50

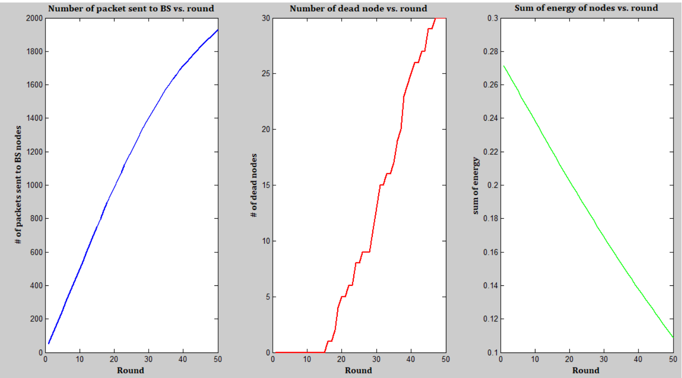

Fig. 5. HYBRID results when number of nodes is 50

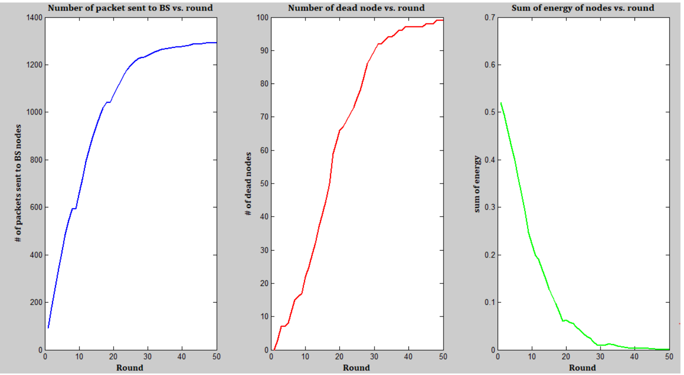

Fig. 6. LEACH results when number of nodes is 100

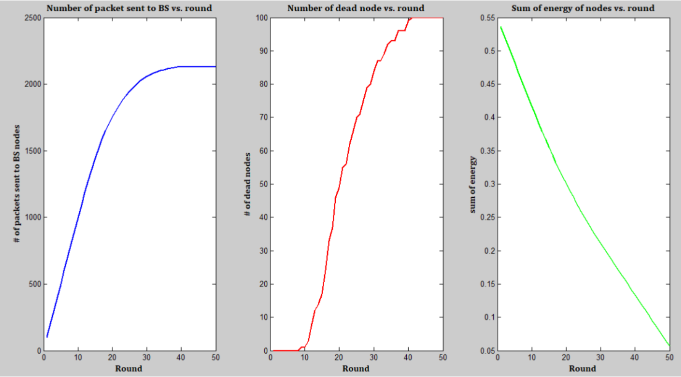

Fig. 7. PSO results when number of nodes is 100

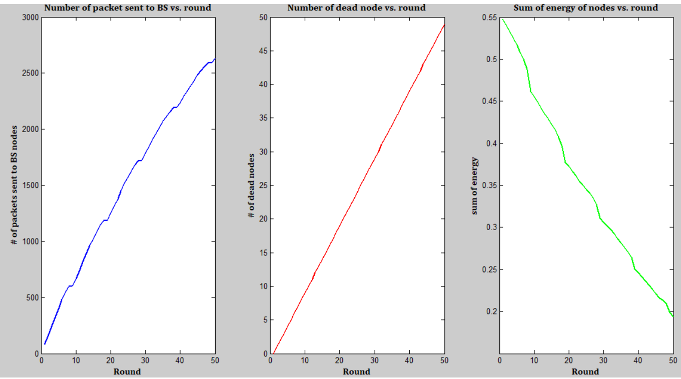

Fig. 8. HYBRID results when number of nodes is 100

VI. Conclusion

The non redundant security algorithm used is simple, memory efficient and protects against various attacks. It prevents node compromise and provides data confidentiality. An hybrid approach using PSO and LEACH was implemented. The protocol runs in two tiers, first one finds the best cluster heads and their associative clusters using LEACH protocol while the second tier solves the problem of the inter-cluster communication by finding the optimal routing path using PSO. The trade-off between the security and energy consumption has been balanced by using the low complexity XOR technique for encryption and Hybrid LEACH- PSO based routing protocol.

References

[1] J. Yick, B. Mukherjee, and D. Ghosal, “Wireless sensor network survey,” *Computer networks*, vol. 52, no. 12, pp. 2292–2330, 2008.

[2] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” in *Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on*. IEEE, 2005, pp. 324–328.

[3] A. Rani and S. Kumar, “A low complexity security algorithm for wireless sensor networks,” in *Power and Advanced Computing Technologies (i-PACT), 2017 Innovations in*. IEEE, 2017, pp. 1–5.

[4] R. Kandpal and R. Singh, “Improving lifetime of wireless sensor networks by mitigating correlated data using leach protocol,” in *Information Processing (IICIP), 2016 1st India International Conference on*. IEEE, 2016, pp. 1–6.

[5] S. Sarangi and B. Thankchan, “A novel routing algorithm for wireless sensor network using particle swarm optimization,” *IOSR Journal of Computer Engineering (IOSRJCE)*, vol. 4, no. 1, pp. 26–30, 2012.

[6] X. Zhang and K. K. Parhi, “Implementation approaches for the advanced encryption standard algorithm,” *IEEE Circuits and systems Magazine*, vol. 2, no. 4, pp. 24–46, 2002.

[7] X. Zhou and X. Tang, “Research and implementation of rsa algorithm for encryption and decryption,” in *Strategic Technology (IFOST), 2011 6th International Forum on*, vol. 2. IEEE, 2011, pp. 1118–1121.

[8] I. C. Trelea, “The particle swarm optimization algorithm: convergence analysis and parameter selection,” *Information processing letters*, vol. 85, no. 6, pp. 317–325, 2003.

[9] R. S. Elhabyan and M. C. Yagoub, “Two-tier particle swarm optimization protocol for clustering and routing in wireless sensor network,” vol. 52. Elsevier, 2015, pp. 116–128.