Multilink Routing in Wireless Sensor Networks with Integrated Approach for Highly Secured Adaptive Energy

Ms. Rucha Kamble
ME in Wireless Communication and Computing
JDCOEM, Nagpur
RTMNU, Nagpur, India
kamble.rucha3@gmail.com

Prof. M.M Baig
ME in Wireless Communication and Computing
JDCOEM, Nagpur
RTMNU, Nagpur, India
mirzammb@gmail.com

Abstract—Now a day's people make use of sensors in order to have a distant communication without any intervention and to avoid the use of wires so that our communication will be mobile, but these sensors suffers a problem of battery drainage. There are various Energy Efficient Protocols for WSN that are being created which aspire to successfully deliver the data packets from sensor node (source) to the Base Station. These protocols have certain parameters like distance to identify the route. These protocols have a considerable amount of energy to find the minimum distance. Our aim is to formulate a protocol which has a target to calculate an efficient path at the same time save the energy of sensors in order to enhance the lifetime of network. In our project we proposed an Optimum Path and Energy Aware Sensor Routing Protocol (OPEASRP) which makes use of load as a parameter for calculation of optimal path and LEACH for conservation of energy of the nodes. At the same time we are providing the strong security to the network for preventing the network from different attacks. The main function of this protocol is for authorized multiple network user. So, with the help of different security parameters the system provides a high security to the wireless sensor network. Energy efficient new algorithm is also used because it is difficult to crack.

***General Terms**: Wireless Sensor Network, Path Finding, Load Balancing*

*****

I. INTRODUCTION

Now a day's Wireless sensor networks are very popular in transmitting data and gathering useful geographical and environmental information.

A wireless sensor network (WSN) consisting of randomly distributed electronic devices make use of sensors to track local or environmental conditions. A WSN system has a gateway that offers non-wired connectivity reverted to the wired world and distributed nodes. A Wireless Sensor Network's nodes consists of various components includes the antenna, power battery, microcontroller, analog circuit, and sensor interface. While using Wireless Sensor Network's radio technology, one must take important trade-offs. In battery-powered devices, higher radio data transfer rates and continuous sensing of nearby radio channel may result in draining battery more often.

To make the battery life better, a node after certain period of time wakes up and transmits data by powering on the antenna and then powering it back off to save energy. Microprocessor trends for WSNs include minimizing power consumption while retaining or enhancing processor's speed. Much like a selected radio, the power usage and its transforming speed trade-off is a primary factor when selecting a processor, for communication. Now days more work is evolving to reduce the power consumption of WSN, but still the results are not that much proven.

While keeping in mind the energy conservation, protocols suggested earlier should also be designed to attain robustness in routing structure. Many paths finding algorithms focus on endorsing the load-balancing technologies to attain the energy-saving effect by real time adjusting the distribution of flow traffic in networks only based on the current-status resources of link and nodes.

This proposed approach has a determination to save the energy of sensor nodes. This approach is a combination of two techniques called Load Balancing and LEACH Algorithm. This suggested approach will definitely give a better output in terms of increasing the efficiency of WSN and save the energy of sensor nodes.

LEACH methodology will form the clusters with the participation of sensor nodes and selects a Cluster Head to forward the communication on behalf of the cluster. The criteria for selecting a cluster head is nothing but the load calculated in the load calculation process. In a cluster the node with lowest load is selected as the Cluster Head (CH). This CH then transfer's the packets to base station (BS).

As you know that a wireless sensor network (WSN) consisting of randomly distributed electronic devices make use of sensors to track local or environmental conditions. A WSN system has a gateway that offers non- wired connectivity reverted to the wired world and distributed nodes. A Wireless Sensor Network's nodes consists of various components includes the antenna, power battery, microcontroller, analog circuit, and sensor interface. While using Wireless Sensor Network's radio technology, one must take important trade-offs. In battery powered devices, higher radio data transfer rates and continuous sensing of nearby radio channel may result in draining battery more often. To make the battery life better, a node after certain period of time wakes up and transmits data by powering on the antenna and then powering it back off to save energy. Microprocessor trends for WSNs include minimizing power consumption while retaining or enhancing. processor's speed. Much like your selected radio, the power usage and its transforming speed trade-off is a primary factor when selecting a processor for communication. Now days more work is evolving to reduce the power consumption of WSN, but still the results are not that much proven. While keeping in mind the energy conservation, protocols suggested earlier should also be designed to attain robustness in routing structure. Many paths finding algorithms focus on endorsing the load-balancing technologies to attain the energy-saving effect by real time adjusting the distribution of flow traffic in networks only based on the current status resources of link and nodes.

Wireless sensor networks are highly distributed network of all small and light weighted nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, relative humidity. Each node of the sensor network consists of three subsystem i.e. sensor subsystem which sense the environment, processing subsystem which performs local computation on the sensed data, and communication subsystem is responsible for message exchange with neighboring sensor node.

II. PRESENT WORK

Many symmetric and asymmetric encryption ciphers have been proposed and developedby researchers. Literature demonstrates symmetric ciphers are more efficient as compared to asymmetric ciphers. Some common symmetric key ciphers are discussed below.

3.1 DES

DES is a 64 bit block cipher It encrypts 64 bits of data at a time using key of length 56 bits. 16rounds of processing are applied to plain text after initial permutation and the last step is to apply final permutation to obtain a 64 bit cipher text. DES uses fiestel structure and its designis an inspiration for many block ciphers. Wuling Ren et. al. in [7] proposed an hybridencryption mechanism based on DES and RSA. RSA is a public key encryption algorithm andused for the encryption of DES's key to be shared between shared and receiver. DES was prone to Brute Force Attack as there are only 2^{56} combinations of key are possible. It was quite easy to crack the DES and making it non-preferable approach for WSN security.

3.2 Triple DES

Triple DES or 3DES was proposed to enhance the security mechanism of DES. Key sizewas extended from 56 bits to 168 bits (56*3). Also it used 3 rounds of DES encryption. 3DEScan be used in two ways either with three keys having 2^{168} possible combinations or with twokeys having 2^{112} possible combinations. Cryptanalysis of 3DES shows that with so manycombinations of key, brute force attack is practically impossible [8]. Large key size makes3DES strongest encryption algorithm, but however it requires a large amount of time andmemory and thus making it an expensive algorithm.

3.3 AES

As per [9] Advance Encryption Standard (AES) also referred as Rijndael cipher is a block cipher with block size of 128 bits and three different key sizes of 128, 192 and 256 bits. AES uses a non-fiestel structure for encryption decryption. Key size depends on the number of rounds which can be 10,12 or 14 for key size of 128,192 or 256 bits respectively. Round keyused by AES is always of 128 bits. As explained in [10] basic Structure of AES is represented in figure 4. First transformation of round is *Substitution* where substitution of bytes is done via using S-box.After a state is substituted another transformation that is applied to state is*Shifting*. Number of shifts of state matrix depends on the row number that can be 0,1,2 or 3. *Mixcolumn* transformation is matrix multiplication where state column is multiplies by a constant matrix. Finally a round key word is added with each state matrix in *Addroundkey* transformation.

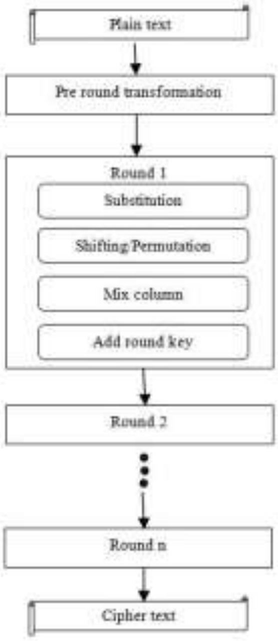

Figure 3. AES Architecture

3.4 RC5

As per [11] RC5 is a potential cipher for data security in WBSN. It is a efficient and flexiblealgorithm where encryption attributes like number of rounds, block size, key length can beadjusted according to the application. As discussed in [12] RC5 uses operations like modulo2word-size addition, bit wise exclusive-or and a cyclic left rotation of word in each round. RC5with short parameter value is susceptible to differential attack; whereas RC5 with large parameters value is time consuming.

Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

III. SIMULATION OUTCOMES

The following are the screen shots acquired during network formation

5.2.1 Deployment of Nodes

Here the assumption is that sensors are placed into a plane and linear surface. The sensors are placed randomly i.e. regardless of their location and sequence. Each Node is equipped with the electronic devices like Transceiver, Battery etc. to initiate the communication by sensing other nodes and forwarding data packets,

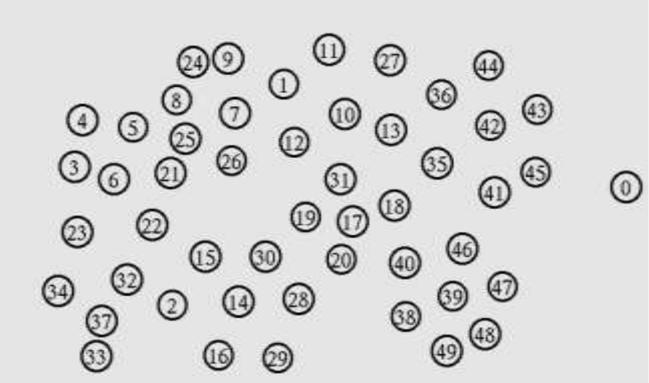

Fig. 1 Screenshot Deployment of Nodes

5.2.2 Forming Clusters and Cluster's Head

To accomplish this, the proposed approach has applied LEACH algorithm in order to form the cluster and select cluster Head the Algorithm is explain in chapter 3. Different colors shows, different clusters. Every cluster Head is marked with CH on the top. The destination node is given as Base_Station.

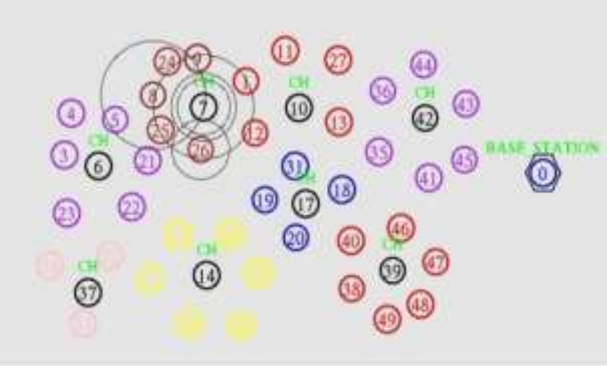

Fig. 2 Screenshot Formation of Cluster and Selecting Cluster Head.

5.2.3 Sensing Neighbors:

In the proposed approach, in order to find the optimal path AODV algorithm is been applied. To send the packet from source to destination every CH is sensing its neighbor by considering the parameters like Distance and Battery power. This process will helps in knowing which path to choose to forward the data packet.

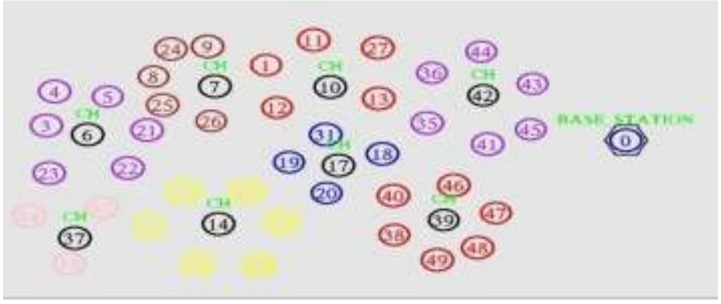

Fig.3. Screenshot Sensing Neighbor.

5.2.4 Selecting Path:

In the proposed approach optimal path has been selected, shown by nodes surrounding by square. The paths have been selected by calculating loads of each and every individual node so that the transmission will be proper and reliable. Calculating the load balance using the below approach:

Load = no of packets released / total number of packets

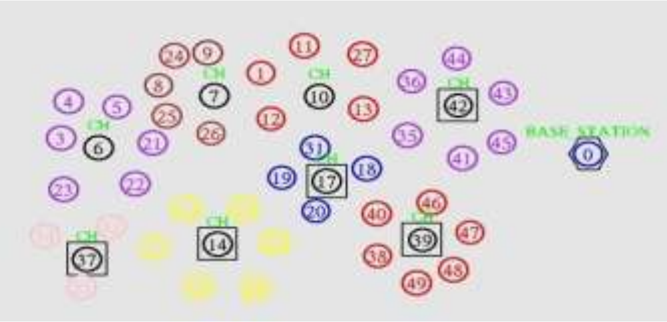

Fig. 4. Selecting the Path

5.2.5 Detection of Malicious Node :-

In the network, it is very difficult to identify that node is malicious or not. But, malicious nodes are detected and that are removed with the help of AP algorithm

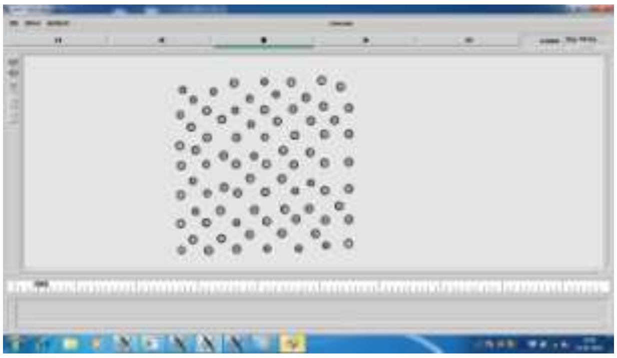

Fig. 5 Detecting the Malicious Node.

.

IV. RESULTS AND CONCLUSIONS

Energy Consumption Graph:

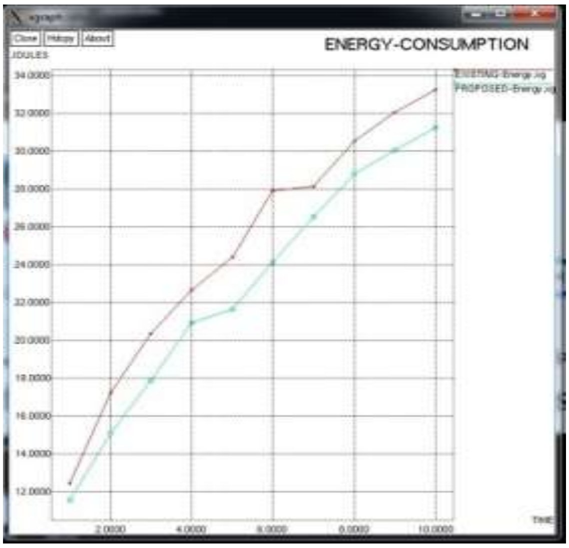

Fig.6 Screenshot Energy Consumption graph (red= existing:: green = our)

The above graph depicts that after using the approach proposed here, the energy consumed by sensor nodes decreased as compared to the existing approach.

Packet Delivery Ratio Graph:

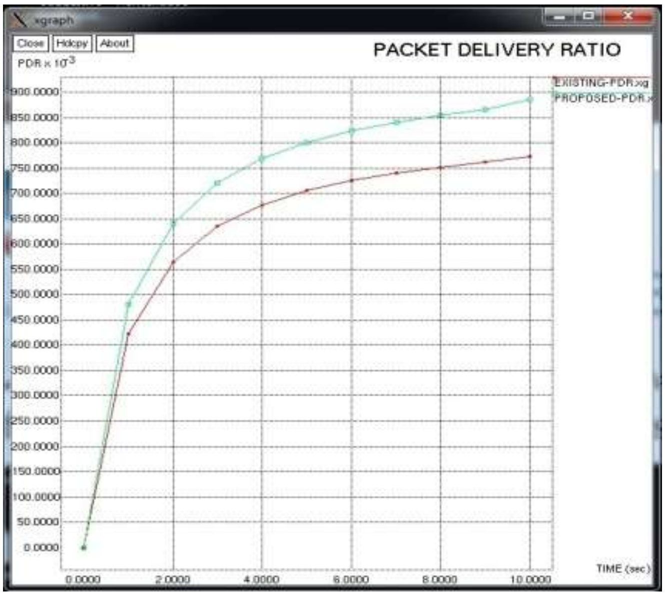

Fig. 7. Screenshot Packet Delivery Ratio (red= existing:: green = our)

The above graph shows that after comparing the existing approach with this proposed approach the packet delivery ratio also gets increase as the ratio of failure of nodes has been decreased.

7. Throughput Graph:

The above graph shows the throughput of the system after applying the proposed approach. As the proposed approach results in less power consumption and increased in packet delivery ratio hence, the throughput of the system is also increased.

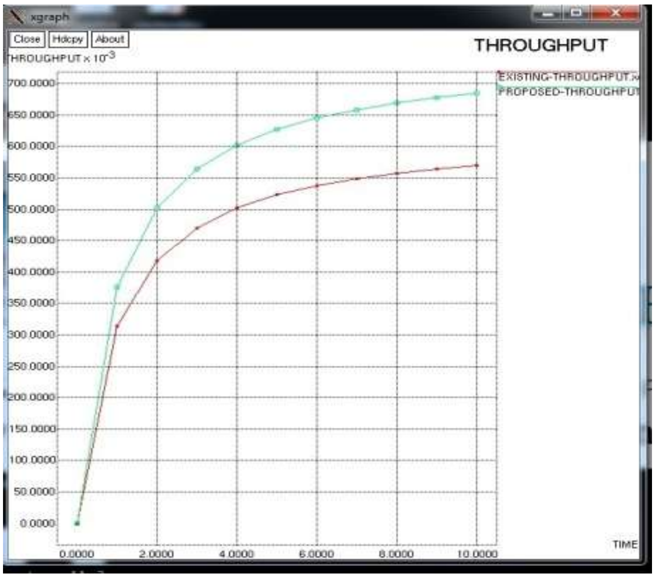

Fig. 8. Screenshot Throughput (red= existing:: green = our)

V. CONCLUSION AND FUTURE SCOPE

Considering such a problem with wireless sensor network in accordance with the security is more complex and challenging in nature and the security vulnerabilities in data discovery and dissemination when used in WSNs. Also, some energy efficient new algorithms (AP) havebeen proposed. Thus, in the future work, we will consider how to ensure data confidentiality in the design of secure and distributed data discovery and dissemination protocols and AP algorithm and the system will maintain the integrity of the data also ensure the performance of the system. We proposed a new symmetric key algorithm (AP) based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack. In this research we will not only going to detect the malicious node from the network, but we will also remove the attacker node from the network, which will make the system muchmore secure and reliable. This will provide us a high security to the wireless sensor networkby detecting and removing the attacker from the network. and optimal path finding and toextend the lifetime of the Sensor node. Here we can conclude that the proposed system will provide the high security. Then by applying energy efficient new algorithm we can encrypt and decrypt the message for the security purpose. This will provide us a high security to thewireless sensor network by detecting and removing the attacker from the network. The analysiswas performed in network simulator (NS2).The project is the successful implementation of an optimal path finding approach which results in saving the energy of sensor nodes which in turn increase the lifetime of a wireless sensor network.This approach will not only make the communication better but it will remove thedrawback of changing battery by reducing the power consumption of the sensor nodes.

The future work will include the placing of Sensor's on a non-planar surface, also with a solution to find a shortest path for transmission.

REFERENCES

[1] Rupika Goyal, Shashikant Gupta, Pallavi Khatri Energy Aware Routing Protocol over Leach on Wireless Sensor Network , International Conference on Computing, Communication and Automation (ICCCA2016), ISBN: 978-1-5090-1666-2/16/$31.00 ©2016 IEEE, pg no. 699-703

[2] Chuanyao Nie, Hui Wu, Wenguang Zheng, Latency and Lifetime-Aware Clustering and Routing in Wireless Sensor Networks, 2016 IEEE 41st Conference on Local Computer Networks, © 2016, Chuanyao Nie. Under license to IEEE. 164 DOI 10.1109/LCN.2016.33

[3] Haibo Zhang and Hong Shen Energy-Efficient Beaconless Geographic Routing in Wireless Sensor Networks IEEE Transactions On Parallel And Distributed Systems, Vol. 21, No. 6, June 2010

[4] D. He, S. Chan, Mohsen, Guizani, H. Yang, "Secure and distributed data discovery and dissemination in Wireless Sensor Network", IEEE Trans. Parallel and distributed system, 2014

[5] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[6] D. He, C. Chen, S. Chan and J. Bu, "DiCode: DoS resistant and distributed code dissemination in wireless sensor networks", IEEE Trans. Wireless Commun., vol. 11, no. 5, pp. 1946-1956, May 2012

[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638-4646, Sept. 2013

[8] Yong-Zhen Li, Ai-Li Zhang, Yu-Zhu Liang Improvement of Leach Protocol for Wireless Sensor Networks 2013 Third International Conference on Instrumentation, Measurement, Computer, Communication and Control

[9] DipakWajgi, Dr. Nileshsingh V. ThakurLoad Balancing Algorithms in Wireless Sensor Network : A Survey IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501

[10] TrianaMugiaRahayu, Sang-Gon Lee*, Hoon-Jae Lee Survey on LEACH-based Security Protocols February 16~19, 2014 ICACT2014