
Ms. Rucha Kamble¹, Prof. M.M Baig²
Department of Computer Science and Engineering, JDCOEM, Nagpur
¹E-mail: kamble.rucha3@gmail.com
²E-mail: 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.

General Terms Wireless Sensor Network, Path Finding, Load Balancing

1. Introduction
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 [9].This paper has a determination of an approach 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 gives 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 [2]. The criteria for selecting a cluster head is nothing but the load calculated in the load calculation process [2]. In a cluster the node with lowest load is selected as the Cluster Head.
Head (CH). This CH then transfer’s the packets to base station (BS) [3]. 2. LITERATURE SURVEY Haibo Zhang and Hong Shen [1] has proposed a novel online routing scheme, called “Energy-Efficient Geographic Routing in Wireless Sensor Networks” (EBGR), which can provide loop-free, fully stateless, energy-efficient sensor-to-sink routing at a low communication overhead without the help of prior neighborhood knowledge, wherein they have established the lower and upper bounds on hop count and the upper bound on energy consumption under EBGR for sensor-to-sink routing, assuming no packet loss and no failures in greedy forwarding. Yong-Zhen Li, Ai-Li Zhang, Yu-Zhu Liang [2] has proposed a hierarchical routing improved algorithm based on the LEACH algorithm (i.e., LEACH-R). The simulation results show that the improved algorithm makes the energy distribution more balanced, and LEACH-R outperforms LEACH-M nearly 20%. In this paper authors has compared and analyze the advantages and disadvantages of the existing technique. Cluster heads receive message and transmit it to the base station directly, the energy consumption is more than ordinary nodes, which leads to dead Based on LEACH protocol, this paper proposes an improved routing optimization algorithm, in order to extend the whole network lifetime.

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. WSNs have a wide range of applications, ranging from monitoring environments, military zones, sensitive installations and remote data collection and analysis. The most important operation in sensor network is data dissemination. It is the process by which queries or data are routed in the sensor network. The data collected by sensor nodes has to be communicated to the base station or to any other node interested in the data. The node that generates data is called a source and the information to be reported is called an event. A node which is interested in an event and seeks information about it is called sink.

Overview
DiDrip consists of four phases, system initialization, user joining, packet pre processing and packet verification. For our basic protocol, in system initialization phase, the network owner creates its public and private keys, and then loads the public parameters on each node before the network deployment. In user joining phase, a user gets the dissemination privilege through registering to the network owner. In packet pre-processing phase, if a user enters to the network and wants to dissemination some data items, he/she will need to construct the data dissemination packets and then send them to the nodes. In packet verification phase, a node verifies each received packet. If the result is positive, it updates the data according to the received packet.

Work in current system
After a wireless sensor network (WSN) is deployed, there is usually a need to update buggy/old small programs or parameters stored in the sensor nodes. This can be achieved by the so-called data discovery and dissemination protocol, which facilitates a source to inject small programs, commands, queries, and configuration parameters to sensor nodes. Data discovery and dissemination protocol for wireless sensor networks (WSNs) is responsible for updating configuration parameters of, and distributing management commands to, the sensor nodes.

Literature Review
3.1. Survey of Existing Methods
D. He, S.Chan, Mohsen Guizani, H.Yang [1],they had proposed the first secure and distributed data discovery and dissemination protocol named DiDrip. It allows the network owners to authorize multiple network users with different privileges to simultaneously and directly disseminate data items to the sensor nodes, it addresses a number of possible security vulnerabilities that they identified. Extensive security analysis show DiDrip is provably secure.
Archan a Tayal, Prachi [2], in this research notes, they proposedApplications of wireless sensor network are increasing day by day. Data nodes in sensor network are easy to capture and confidential data of sensor nodes can be accessed by eavesdropper. Security has always been troublesome in the wireless communication. Cryptography algorithms are kernel of the WSN security. They present 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. The features are time taken by algorithm for different key size and number of rounds along with the comparative analysis of proposed algorithm with AES on various parameters to prove its efficiency.
D. He, C. Chen, S. Chan and J. Bu [3] they proposed the development of a secure and distributed code dissemination protocol named DiCode is done. A salient feature of DiCode is its ability to resist denial-of-service attacks which have severe consequences on network availability. Further, the security properties of this protocol are demonstrated by theoretical analysis. To verify the efficiency of the proposed approach in practice, also implement the proposed mechanism in a network of resource-constrained sensor nodes.

Haibo Zhang and Hong Shen [1] has proposed a novel online routing scheme, called “Energy-Efficient Beaconless Geographic Routing in Wireless Sensor Networks” (EBGR), which can provide loop-free, fully stateless, energy-efficient sensor-to-sink routing at a low communication overhead without the help of prior neighborhood knowledge, wherein they have established the lower and upper bounds on hop count and the upper bound on energy consumption under EBGR for sensor-to-sink routing, assuming no packet loss and no failures in greedy forwarding. Yong-Zhen Li, Ai-Li Zhang, Yu-Zhu Liang [2] has proposed a hierarchical routing improved algorithm based on the LEACH algorithm (i.e., LEACH-R). The simulation results show that the improved algorithm makes the energy distribution more balanced, and LEACH-R outperforms LEACH-M nearly 20%. In this paper authors has compared and analyze the advantages and disadvantages of the existing technique. Cluster heads receive message and transmit it to the base station directly, the energy consumption is more than ordinary nodes, which leads to dead nodes.

Prolong network lifetime, decrease the redundancy of data packets, reduces the rate of energy consumption etc. Triana Mugia Rahayu, Sang-Gon Lee*, Hoon-Jae Lee[4] has proposed to strengthen LEACH protocols. Those protocols are SLEACH, SecLEACH, SC-LEACH, Armor LEACH and MS-LEACH. They described the security analysis of SLEACH, SecLEACH, SC-LEACH, Armor LEACH and MS-LEACH. They had also provided some possible solution to some pointed drawbacks. The findings about previous drawbacks also directs them, that it is needed to devise efficient secure protocol for WSN that combines both secure routing protocol and secure data aggregation protocols together. Rachel Cardell-Oliver1, Keith Smettem2 Mark Kranz1 and Kevin Mayer [5] has proposed the design and test of a sensor network that successfully meets the goal of reactivity, and that demonstrates satisfactory robustness and network lifetime. Improving the performance of the network is the subject of ongoing work. The long term aim of their research is to develop components for sensor networks that can be simply combined to create reactive, long lived networks for a variety of environmental monitoring applications including irrigation in agriculture or urban settings, monitoring of water catchments and dry-land salinity management. They have described the design and implementation of a novel reactive sensor network for monitoring soil moisture and evaluated the reactivity, robustness and longevity of the network in the field. The Pinjar network meets the goal of providing useful data on dynamic responses of soil moisture to rainfall. Future work will focus on addressing the limitations of the current prototype in robustness of packet delivery and network longevity, and in guaranteeing network response to events of interest.

2. Objective
The objective of the proposed system is,

1. Finding approaches and also a proposed solution in order to find a optimal path by saving the energy of wireless sensor nodes.
2. Our objective is to identify the optimal set of routes to deliver messages from sources to sinks.
3. To improve the performance of the network by enhancing the lifetime of the sensor nodes and providing the strong security to the network.
4. To provide the high security to WSN without compromising the performance of system.
5. Detecting and removing the attacker from the network.
6. Maintaining the security and integrity of data.

Research methodology to be employed
In this research we are proposing two different mechanisms one for improving the Energy consumption of the Sensor Node and to find the optimal path between sender and receiver and other is to provide the security to the network a new symmetric key algorithm (AP) is proposed.

Proposed Algorithm
Load balancing can be used to extend the lifetime of a sensor network by reducing energy consumption. Load balancing using clustering can also increase network scalability. Wireless sensor network with the nodes with different energy levels can prolong the network lifetime of the network and also its reliability. Clustering has numerous advantages like it reduces the size of the routing table, conserve communication bandwidth, 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. We are proposing the 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 proposed algorithm new symmetric key algorithm, which is based on shuffling, substitution and shifting to depict a security scheme for WSN which is energy efficient as well as difficult to crack.

Modules
Module 1. Wireless Sensor Network Formation
In this module designing of complete wireless sensor network will be done, and the number of Sensor Nodes, Storage Node and Sink node, and then interrelate them to form the network.

Module 2. Communication in Wireless Sensor Network
Once, designing of Wireless Sensor Network is completed, then the next step is to have the communication between all the nodes, storage node and sink node. The communication in the sense there will be transmission of the data amongst different nodes in the node.

Module 3. Data Discovery and Dissemination
The proposed module will emphasize on distribution of data discovery and dissemination protocols and implementation of the functional requirements of such protocols, and set their design objectives. Also, identify the security vulnerabilities in existing data discovery and dissemination protocols.

Module 4. Providing the Security to WSN
The proposed module is a block cipher symmetric key algorithm. The set of operation known as 3S are shuffling, substitution and shift left those are to be applied to the plain text in each round. Rounds can vary from 2^0 to 2^10. Plain Text could be of any length. Though it is a block cipher but no padding is required in the proposed algorithm.

Module 5. Data Discovery and Dissemination
Calculate the load and distance of all the sensor nodes, based on load and distance calculate the optimal path between source and destination.

Module 5. Result Analysis
Compare the results of proposed system with the existing system.

Shuffling:
In this, algorithm initially generates a permutation table using P-box of size 48 bits to shuffle the plain text. Thus, creating a key space of size 48 bits i.e. 1.2414e + 061 which is sufficiently large enough for the intruder to crack. To elaborate working of algorithm an example is considered with key of 16 bits.

Substitution:
Substitution is performed by using Vigenere Cipher. Vigenere Cipher is a polyalphabetic substitution where text is encrypted using a series of additive cipher. An additive cipher is a traditional cipher where text is shifted ahead to a particular number. Text ‘M’is substituted to ‘U’ for additive key = 8.

Shift:
Cipher text created in previous step is applied a circular shift by a certain number of times, and this number of shift depends upon the key k2 used by vigenere cipher. Key k3 for circular left shift is the leftmost digit of key k2,k3 = leftmost (k2) In the given example k3 = 9 and generated final cipher text.

Expected Outcome
1. We will ensure the design of secure and distributed data discovery and dissemination protocol.
2. We will ensure the optimal path finding in the network.
3. We will ensure the energy saving of the Sensor nodes and so will extend the lifetime of Sensor Network.
4. We will ensure the data confidentiality in the design of secure and distributed data discovery and dissemination protocol.
5. We will verify the security parameter for wireless sensor network, to maintain the integrity of data.
6. System will not only provide the high security to network but also improves the performance of the system.
7. We will analyze the throughput of system, energy consumption, key size, CPU time.

Conclusion
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) have been 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 much more secure and reliable. This will provide us a high security to the wireless sensor network by detecting and removing the attacker from the network, and optimal path finding and to extend 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.

References