ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Energy Efficient Architecture Using Cluster Based Multipath Routing in Large Scale Wireless Sensor Networks

Mohammad Sirajuddin[1], Md Sallauddin[2]

Assistant Professor, Department of Computer Science and Engineering, VGSE, Karimnagar, Telangana, India [1]

Assistant Professor, Department of Computer Science and Engineering, SR, Warangal, Telangana, India [2]

ABSTRACT: In recent era of Wireless Technology, energy efficient design and latest wireless technologies have enabled new exciting applications for wireless devices. These types of applications covers a wide range including real time and streaming video and audio delivery, transfer of large amount of data from one device to another. These applications require high performance on the network, they usually suffering from resource constraints. Wireless devices are often having limited energy resource because nodes are battery operated. This makes application with limited bandwidth & making the transfer error prone WSNs are multi hop networks, which depend on the intermediate nodes to relay the data packet to the destination. These nodes are equipped with lesser memory, limited battery power, little computation capability, small range of communication and need a secured and e client routing path to forward the incoming packet. In this paper, we propose a secure cluster based multipath routing protocol (SCMRP). Researchers have proposed clustered sensor networks to increase the efficiency (i.e. increase system throughput, save energy and decrease system delay by data aggregation) and multipath sensor networks to increase the resilience and reliability of the network. The SCMRP is the combination of these two sensor networks; therefore, it provides efficiency as well as reliability and the proper use of cryptographic algorithm provides client security to the sensor network. SCMRP provides security against various attacks like altering the routing information, selective forwarding attack, sinkhole attack, wormhole attack, Sybil attack etc. Further, we have provided a brief analysis to various issues related to key management, orphan nodes, security and energy e ciency.

KEYWORDS: Secure routing, wireless sensor networks, multi-path, clustering, resilience, security.

I. INTRODUCTION

In recent years we have seen growth of wireless devices including cellular phone, mobiles, laptops and personal digital assistants. The advances in the wireless technology are also one of the major motivations for the growth of the wireless devices or mobile computing. And for this, basically we would like the Wireless Sensor Network to perform its functionality as long as possible.

A number of routing protocols have been proposed for WSN [2, 3, 4]. Few of them are cluster based. Two of the most well known hierarchical protocols are LEACH, and PEGASIS. Both of these show significant reduction in the overall network energy over other non-clustering protocol.

Hierarchical routing protocols designed to reduce energy consumption by localizing communication within the cluster and aggregate data to reduce transmissions to the BS. Leach is considered as the most popular routing protocol that use cluster based routing in order to minimize the energy consumption; Following section describes LEACH protocol, its architecture, analysis & its simulation.
The growth of microwave devices, wireless communication and microprocessor technologies devised to the small, low power and low cost sensor node. These self-organized sensor nodes form multi hope networks, called wireless sensor

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

net-works (WSNs). WSNs are very different than Mobile ad hoc networks (MANETs) in terms of architecture, application and resource capacity. So that the protocols which generally used in MANET, we can't apply directly to the WSN. Therefore in the last one decade researchers are continuously working to enhance efficiency and security of wireless sensor networks. Sensor networks have many applications from the field of medical to battle field and from the homeland security to earthquake monitoring.

The characteristics of sensor networks and application requirements have a decisive impact on the network design objectives in term of network capabilities and network performance Network Characteristics As compared to the traditional wireless communication networks such as mobile ad hoc network (MANET) and cellular systems, wireless sensor networks have the following unique characteristics and constraints:

Dense sensor node deployment: Sensor nodes are usually densely deployed and can be several orders of magnitude higher than that in a MANET.

Battery-powered sensor nodes: Sensor nodes are usually powered by battery and are deployed in a harsh environment where it is very difficult to change or recharge the batteries.

Severe energy, computation, and storage constraints: Sensors nodes are having highly limited energy, computation, and storage capabilities.

Self-configurable: Sensor nodes are usually randomly deployed and autonomously configure themselves into a communication network.

Unreliable sensor nodes: Since sensor nodes are prone to physical damages or failures due to its deployment in harsh or hostile environment.

Data redundancy: In most sensor network application, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

Application specific: A sensor network is usually designed and deployed for a specific application. The design requirements of a sensor network change with its application.

Many-to-one traffic pattern: In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.

Frequent topology change: Network topology changes frequently due to the node failures, damage, addition, energy depletion, or channel fading.

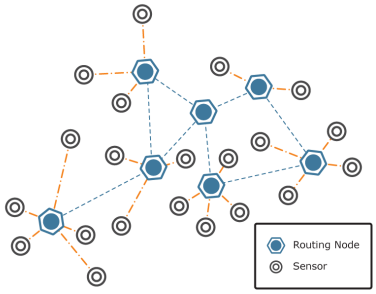


Fig 1.1

Figure 1.1 shows an example of the working of directed diffusion When interests fit gradients, paths of information flow are formed from multiple paths and then the best paths are reinforced so as to prevent further flooding according to a local rule. In order to reduce. The communication costs, data are aggregated on the way. The goal is to find a good aggregation tree which gets the data from source nodes to the BS. The BS periodically refreshes and re-sends the

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

interest when it starts to receive data from the source(s). This is necessary because interests are not reliably transmitted throughout the network.

Most sensor networks are application specific and have different application requirements. Thus, all or part of the following main design

Small node size: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers, reducing node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.

Low node cost: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, reducing cost of sensor nodes is important and will result into the cost reduction of whole network.

Low power consumption: Since sensor nodes are powered by battery and it is often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

Scalability: Since the number sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

Self-configurability: In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

Adaptability: In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.

Fault tolerance: Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self testing, self-calibrating, self-repairing, and self-recovering.

Security: A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

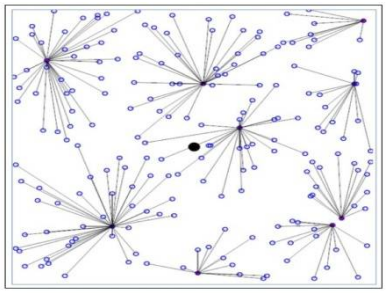


Fig 1.2

Figure 1.2 shows working of the first category of routing protocols are the multi hope flat routing protocols. In flat networks, each node typically plays the same role and sensor nodes collaborate together to perform the sensing task. Due to the large number of such nodes, it is not feasible to assign a global identifier to each node. This consideration has led to data centric routing, where the BS sends queries to certain regions and waits for data from the sensors located in the selected regions. Since data is being requested through queries, attribute-based naming is necessary to specify the properties of data. Early works on data centric routing, e.g., SPIN and directed diffusion] were shown to save energy through data negotiation and elimination of redundant data. These two protocols motivated the design of many other

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

protocols which follow a similar concept. In the rest of this subsection, we summarize these protocols and highlight their advantages and their performance issues

II. CLUSTER BASED ROUTING

In WSNs, broadcasting is the important process for data transmission. Broadcasting is the process in which a source node transmits a message to all other nodes in the network. Clustering is one of the methods for Broadcasting. Our main concern is only about clustering because LEACH is using this. LEACH (Low Energy Adaptive Clustering Hierarchy), a clustering-based protocol that utilizes randomized rotation of local cluster based station (cluster-heads) to evenly distribute the energy load among the sensors in the network. LEACH uses localized coordination to enable scalability and robustness for dynamic networks, and incorporates data fusion into the routing protocol to reduce the amount of information that must be transmitted to the base station.

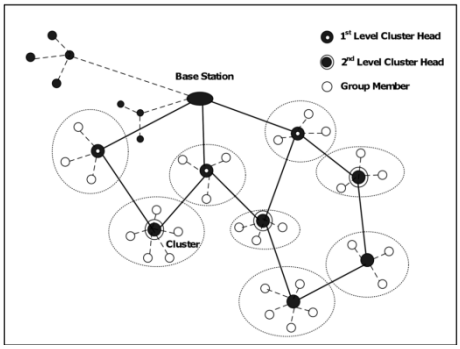


Fig 1.2

Intra-cluster communication is performed by TDMA. Each parent node polls its direct children and forwards the data to its parent node until the data reaches the CH. The parent node may aggregates several data packets from its children together with its own data into one packet. For inter-cluster communication, the CHs poll their first-level children, including their own data, and transmit to the BS. The following is the advantages of DWEHC: (1) Like HEED, it is a fully distributed clustering method that is based on a function of the sensor's energy reserve and the proximity to the neighbours for CH election; (2) Considering energy reserves in CH election, DWEHC generates more well balanced CHs distribution and achieves significantly lower energy consumption in intra-cluster and inter-cluster routing than HEED; (3) The clustering process of DWEHC terminates in a few iterations, and does not depend on network topology or size. Some disadvantages of DWEHC are summarized as follows: (1) Similar to LEACH, single-hop inter-communication, directly from CHs to the BS, is performed in DWEHC. Thus DWEHC may result in significant amount of energy consumption, and is not applicable to large-region networks; (2) In the process of cluster formation, the iterative nature in both DWEHC and HEED produces a relatively high control message overhead compared to other protocols

III. RELATED WORK

There are a huge number of routing protocols present for sensor networks. First time these routing protocols were presented in an organized way by Al-Karaki and Kamal[1], this survey covered almost all aspect of routing protocol, classification and architecture. But all these basic protocols have been implemented without the security. Karlof et al.[7] describe the attacks on di erent routing protocols and provide the countermeasures, which is the base of the many research

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

LEACH[4] is the first and very popular concept of clustered routing without any security. SecLEACH provides an e cient solution for secure communication in LEACH with the help of *random key pre-distribution* and TESLA and over-comes some of the attacks. Again to provide e effective solution for secure communication in LEACH, RLEACH has been introduced with improved random key pre-distribution scheme.

Some work has been done in secure hierarchical routing protocol; this paper described energy e client hierarchical routing protocol with group key management scheme, but when changing the cluster head all group keys (i.e. inter cluster and intra cluster) have to calculate again, is an overhead associated with this protocol. NHRPA is also an approach towards secure hierarchical routing which provide security under node compromise attack. Security against exterior adversary and inner compromised nodes by gene and reputation management tools with extra burden of computation and communication.

All the hierarchical routing protocol has been implemented with the efficiency in mind. If once, we leave the issue of security, there are some other issues exist in clustering protocol like; orphan nodes problem and multi hop path (from the cluster head to the base station). In this paper we overwhelmed these two problems.

There are many multipath routing protocols, exist, which increase resilience and reliability at the expense of in-creased energy consumption, extra c generation and overhead of maintaining the alternative paths. In this paper, we overcome these problems with security as a main issue.

3.1 LEACH Phases:

This protocol is divided into rounds; as shown in Figure 3, each round consists of two phases;

(i) Set-up Phase (ii) Steady Phase

3.1.1 Set-up Phase:

Set-up phase is further divided into 2 parts:

1. Advertisement Phase
2. Cluster Set-up Phase

LEACH forms clusters by using a distributed algorithm where nodes make autonomous decisions without any centralized control.

As shown in Figure 4, In the Advertisement Phase, CHs inform their neighborhood with an advertisement packet that they become CHs. Non-CH nodes pick the advertisement packet with the strongest received signal strength.

Each node decides independent of other nodes if it will become a CH or not.

This decision is made by looking into account when the node served as a CH for the last time (means the node that hasn't been a CH for long time is more likely to elect itself than nodes that have been a CH recently). This is done according to a threshold value, T (n).

The threshold value depends upon the desired percentage to become a cluster-head- p, the current round r, and the set of nodes that have not become the cluster-head in the last 1/p rounds, which is denoted by G. Based on all messages received within the cluster, the CH creates a TDMA schedule, pick a CSMA code randomly, and broadcast the TDMA table to cluster members every node wanting to be the cluster-head chooses a value, between 0 and 1.

If this random number is less than the threshold value, T (n), then the node becomes the cluster- head for the current round.

Then each elected CH broadcasts an advertisement message to the rest of the nodes in the network to invite them to join their clusters.

Based upon the strength of the advertisement signal, the non-cluster head nodes decide to join the clusters.

In the set-up phase, the cluster head nodes are randomly selected from all the sensor nodes and several clusters are constructed dynamically.

Following flowchart shows the procedure for the set-up phase:

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

IV. STEADY PHASE

Steady phase is further divided into 2 parts:

1. Schedule Creation
2. Data Transmission

Figure 5 shows the flowchart for the steady phase.

Once the nodes have elected themselves to be cluster heads the cluster head nodes must let all the other nodes in the network know that they have chosen this role for the current round.

To do this each cluster head node broadcasts an advertisement message ADV using a non persistent carrier sense multiple access CSMA. This message is a small message containing the nodes ID and a header that distinguishes this message as an announcement message. Each non cluster head node determines to which cluster it belongs by choosing the cluster head, that requires the minimum communication energy based on the received signal strength of the advertisement from each cluster head.

After each node has decided to which cluster it belongs, it must inform the cluster head node that it will be a member of the cluster. Each node transmits a join request message (Join_REQ) back to the chosen cluster head using a non persistent CSMA. After schedule creation sub phase, the CH knows the number of member nodes and their IDs. Based on all messages received within the cluster, the CH creates a TDMA schedule, pick a CSMA code randomly, and broadcast the TDMA table to cluster members.

After that Data Transmission phase begins. Nodes send their data during their allocated TDMA slot to the CH. This transmission uses a minimal amount of energy (chosen based on the received strength of the CH advertisement) the radio of Each non-CH node can be turned off until the nodes allocated TDMA slot. This will minimize energy dissipation in nodes. once all the data has been received

V. SIMULATION & RESULT

5.1 Simulation Environment

The simulation experiment is carried out in LINUX (Ubuntu 10.10). The detailed simulation model is based on network simulator-2 (ver-2.34), is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver, to create the statistical data track file and so on.

The implementation software of LS-LEACH was carried using network simulator NS-2. NS-2.34 version was used in this implementation and simulation. NS2 is open source software under GPL (general public license). Moreover, NS2 is built in C++ and the interface is in OTcl language which is an object oriented extension of TCL language. Further, the operating system environment of the simulation was Linux Ubuntu 10.04 LTS installed on system with 2.5 GHz Intel Core 2 Duo and 4 GB memory.

The implementation of LS-LEACH was executed by adding new parameters and functions to the existing LEACH in NS2. Most of the changes were done in the source files of LEACH which are located in the ns-2.34 (as in version 2.34) directory in folder ‘mit’. Other changes were also done in different files for the purpose of the linking of the TCL and C++ as TCL language is used as the interface for NS2 and OTcl is liking between TCL and C.

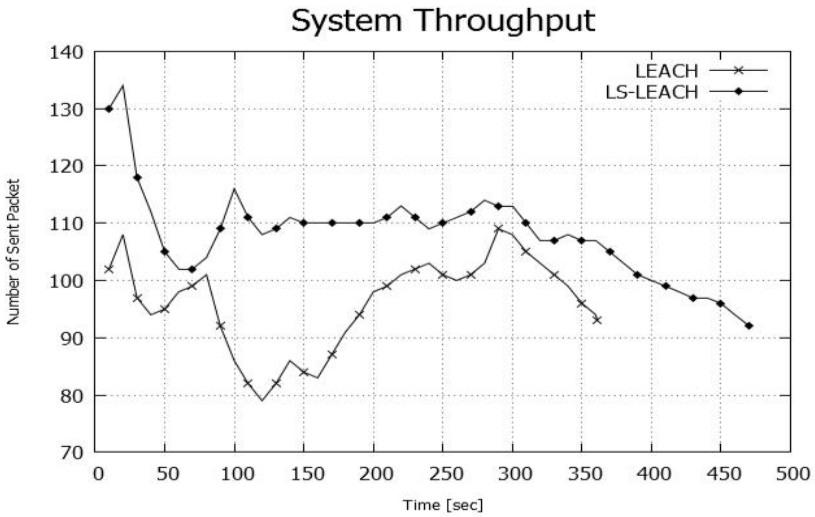
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

5.2 System throughput



1. Fig. 5.1

Fig. 5.1 shows the system throughput comparing between the classical LEACH protocol, and the proposed LS-LEACH. The proposed protocol has better performance because it tries to mitigate the ideal listening by putting the nodes in sleeping state which reduce the power consumption allowing the nodes to live longer and to reduce the collisions. The normal Leach protocol stopped performing because all the nodes died at time 360 which is after 19 rounds. However, the proposed protocol kept performing until time 475 which is after 24 rounds.

5.2 Energy Consumption

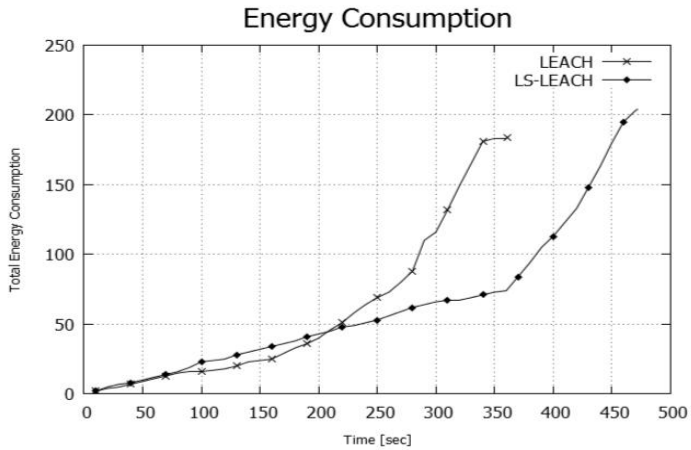


Fig 5.2

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Fig 5.2 Comparing the energy consumption between normal LEACH and leach with security in Fig. 5, we find the proposed protocol has less power consumption. As a result, normal LEACH lasted until time 364 and the proposed protocol lasted until time 371. The increase of power consumption in LEACH protocol started at time 210 with the loss of the first node. As a result, the other nodes faced more load due to the increase of power consumption which reduced the network life. On the other hand, the proposed protocol lost the first node at time 360. This reduced the power consumption and increased the network life time.

REFERENCES

1. M. Bani Yassein, A. Al-zou'bi, Y. Khamayseh, W. Mardini. Application-Specific Protocol Architectures for Wireless Networks. International Journal of Digital Content Technology and its Applications, Volume 3, Number 2, June 2009.
2. Baiping Li1, Xiaoqin Zhang. Research & Improvement of LEACH Protocol for Wireless Sensor Network. International Conference on Information Engineering, 2012.
3. Dilip Kumar, Trilok C. Aseri, R.B. Patel. EEHC: Energy efficient heterogeneous clustered scheme for wireless sensor networks. Computer Communications 32 (2009) 662–667.
4. Lu Xiang, Q. and Y. Tian. An efficient heuristic control algorithm for wireless sensor networks. in Educational and Network Technology (ICENT), 2010 International Conference on. 2010.
5. Yong, H. Design and Realization of Wireless Sensor Network for Vegetable Greenhouse Information Acquisition. in Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on. 2010.
6. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. Comput. Netw. 2002, 38, 393–422.
7. Haas, Z.J.; Halpern, J.Y.; Li, L. Gossip-Based Ad Hoc Routing. In Proceedings of the 19th Conference of the IEEE Communications Society (INFOCOM), New York, NY, USA, 23–27 June 2002; pp. 1707–1716.
8. Sustainable Wireless Sensor Networks; Seah, W., Tan, Y. Eds.; InTech Open Access Publisher: Rijeka, Croatia, 2010