Engineering Universe for Scientific Research and Management
(International Journal)
ISSN(ONLINE) : 2319-3069
Vol. 7 Issue 1
January 2015

Cluster based Energy Efficient Routing Protocol for Wireless Sensor Network

Harsha Mishra[1], Prof. Vaibhav Kumar[2], Prof. Sini Shibu[3]
Department of Computer Science & Engineering
NRI, Bhopal[1,2,3]
harshamishra2004@rediffmail.com[1]

***Abstract*- Wireless network is a most famous approach in these days. Wireless Sensor network is one of the popular applications of wireless network. The sensor network uses some kind devices. There are number of devices are used in the network area. These devices are use to collect the data from sensing the environment. Due to large number of devices the input data collection is also large. To reduce processing of this data there is a need to narrow the processing space. This is knows as data aggression. As there are many approach used in classification of data of sensors**
This paper has proposed an approach by which the energy can be saved in sensor network. The results shows the proposed method gives the batter results.

Keywords- sensor Network, AODV, Routing Protocols

I. WIRELESS NETWORK

A Network is use to connect the devices for sending and receiving the data. To install any network there are three basic needs. These are 1) Computers 2) Connecting Media and 3) Protocol. As the network is a way to provide communication between two or more than two devices. Whether, wireless network uses radio waves to connect devices such as laptops to the Internet and to your business network and its applications. When you connect a laptop to a WiFi hotspot at a cafe, hotel, airport lounge, or other public place, you're connecting to that business's wireless network. Using this approach the wireless LAN can create to establish it in a required area[1].

The figure 1 shows the simple scenario in which there are many nodes which are connected with the wireless medium. This wireless medium may created by the centralized device like router, switch or a computer.

The 802.11 standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance, an industry standard group promoting interoperability among 802.11 devices. The 802.11 standard offers two methods for configuring a wireless network ad hoc and infrastructure. Earlier there was a discussion that Wireless network refers to a network, in which all the devices communicate without the use of wired connection. Wireless networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network [2].

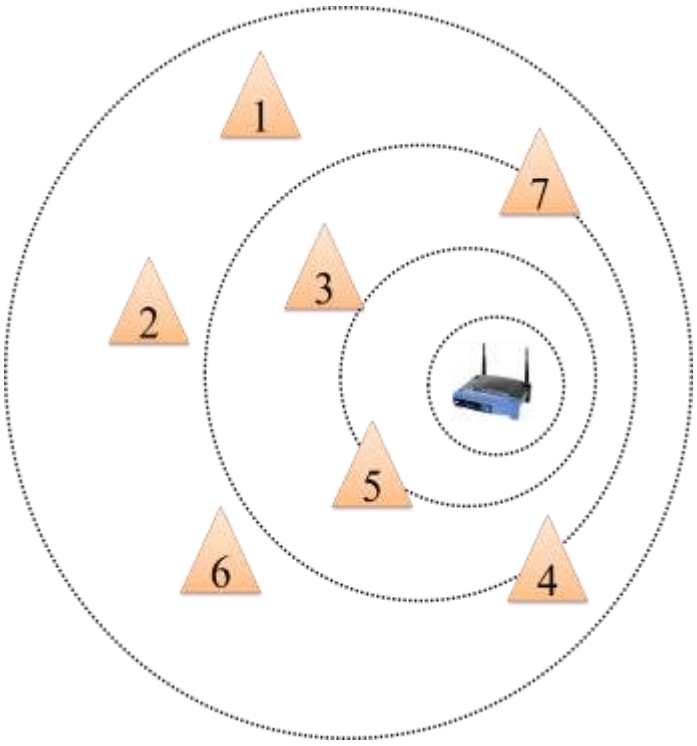

Figure 1: Wireless Network

II. SENSOR NETWORK

Sensor networks are dense wireless networks of small, low-cost sensors, which collect and disseminate environmental data. Wireless sensor networks facilitate monitoring and controlling of physical environments from remote locations with better accuracy. They have applications in a variety of

fields such as environmental monitoring, military purposes and gathering sensing information in inhospitable locations. Sensor nodes have various energy and computational constraints because of their inexpensive nature and ad-hoc method of deployment.

Previously, sensor networks consisted of small number of sensor nodes that were wired to a central processing station. However, nowadays, the focus is more on wireless, distributed, sensing nodes. When the exact location of a particular phenomenon is unknown, distributed sensing allows for closer placement to the phenomenon than a single sensor would permit. Also, in many cases, multiple sensor nodes are required to overcome environmental obstacles like obstructions, line of sight constraints etc. In most cases, the environment to be monitored does not have an existing infrastructure for either energy or communication. It becomes imperative for sensor nodes to survive on small, finite sources of energy and communicate through a wireless communication channel.

The emerging field of wireless sensor networks combines sensing, computation and communication into a single small unit. With advanced network protocols networking, these devices form a sea of connectivity extends the reach of cyberspace into the physical world. When water flows to fill each room of a ship submerged mesh network connectivity will look and operate any type of communication data as possible jumping from one node to another in search of his destiny. While the capacity of any single device are minimal, the composition of hundreds of devices offers radical new technological possibilities.

III. SENSOR NETWORK ROUTING

Routing in sensor networks involves finding a path from the source to the destination, and delivering packets to the destination nodes while nodes in the network are moving freely [31]. Due to node mobility, a path established by a source may not exist after a short interval of time. To manage with node mobility nodes need to maintain routes in the network. Depending on how nodes establish and maintain paths, routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid, and location-based categories.

If a routing protocol is needed, why not use a conventional routing protocol like link state or distance vector? They are well tested and most computer communications people are familiar with them. The main problem with link-state and distance vector is that they are designed for a static topology, which means that they would have problems to converge to a steady state in an ad-hoc network with a very frequently changing topology.

Link state and distance vector would probably work very well in an sensor network with low mobility, i.e. a network where the topology is not changing very often. The problem that still remains is that link-state and distance-vector are highly dependent on periodic control messages [29]. As the number of network nodes can be large, the potential number of destinations is also large. This requires large and frequent exchange of data among the network nodes [31]. This is in contradiction with the fact that all updates in a wireless interconnected sensor network are transmitted over the air and thus are costly in resources such as bandwidth, battery power and CPU. Because both link-state and distance vector tries to maintain routes to all reachable destinations, it is necessary to maintain these routes and this also wastes resources for the same reason as above [33]. Another characteristic for conventional protocols are that they assume bi-directional links, e.g. that the transmission between two hosts works equally well in both directions. In the wireless radio environment this is not always the case.

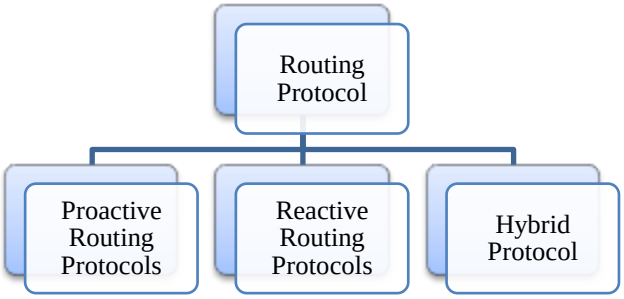

Figure 2 Protocol Used in sensor network

IV. LEACH ALGORITHM

As a new acquisition and data processing technology, wireless sensor networks (WSN) has a wide range of applications in military, environmental monitoring, smart furniture and space exploration and so on. A wireless sensor network can be described as a car system consists of many nodes sensors designed to communicate with each other wirelessly by radio, and can collaborate in real-time monitoring, data collection and collect information from various environmental factors or tracking objects and transfer

the information to the base station.It not need a fixed network support and quick work, survival and other characteristics, so it has a good prospect of application. Until now, research on wireless sensor networks in general through two steps, the first step is essentially for the second network node level questions, the main research in this stage include network layer protocol and the MAC layer according to the energy optimization, location technology nodes, clock The synchronization technology and data fusion technology. Study of routing protocols in wireless sensor networks is one of the hot topics at this stage. Leach protocol is the first protocol hierarchy routes proposed data fusion is milestone importance of routing protocols reunion. so much Hierarchical routing protocols are based on improving

LEACH Protocol. So when wireless sensor networks go slowly in our lives is of great importance to leaching research protocol. based on a clustering protocol that uses random rotation base stations in the cluster (local cluster heads) to evenly distribute the energy load among the sensors in the network Data aggregation reduces the amount of information transmitted to the base station; significant reduction in power dissipation calculation is much cheaper than communication it can reach up to a factor of 8 reduction in power dissipation compared to the conventional routing protocol

Standard protocols may not be optimal for static sensor networks - direct transmission, MTE minimal power transmission, multi-hop routing, and grouping.

An advantage of the coordination and control of the creation and operation of the group is to have located Smal transmission distances. Here each node decides whether to become a center head for the current round of step advertising

V. ISSUE IN SENSOR NETWORK

We mainly focus on the distributed (and local) designing algorithms for these problems, where individual nodes perform their own algorithms for computing solutions to a global problems. A distributed algorithm is one in which the nodes individually execute the same algorithm and make decisions accordingly without knowing the general network topology. However, in some distributed algorithms, it is permissible that the nodes can learn some overall information (for example, the number of sensors in the Network and / or the maximum level of the underlying curve). A stronger version of distributed algorithm is known as the local algorithm. Unofficially, a local algorithm, allows a node to communicate only with their neighbors, which are plus a constant jump away to make decisions during the execution of the algorithm

VI. PROPOSED METHODOLOGY

ESAODV is an proactive node disjoint multipath routing protocol. In ESAODV, WSN is assumed to consist of several steps Sti = 1, i 2, ..., l based on the number of hops between the source and destination. The sink is a node St0 zero. Each node can communicate with the receiver node is St1. We assume that a node can communicate with nodes on the same stage Sti Sti Sti and the next step + 1 but cannot communicate with Sti-1 nodes. This avoids looping paths. Initially, all network nodes have a very high value of the hop count with the exception of the receiving node. Initially, all nodes have their residence above the threshold energy level energy. Multiple paths from all nodes to the sink is generated in the construction phase of the road. In the process of building the packages Route (RCON) are exchanged between nodes. Each sensor node transmits the packet once RCON and maintains its own routing table. If there is no path to the sink node through the RCON received packet, then the node processes the packet RCON. If the path to flow from this node is already available in the routing table of the node, then the number of hops the packet is checked. If the hop number of packets is less than the value of the node and its residual energy jump is greater than the power threshold value, then it is RCON; otherwise the packet is discarded. The node receiving the RCON packet, updates the RCON packet. RCON is updated with incremental number of hops by one, updates the node ID before adding the node identifier in the way. The node receiving the RCON packet updates its routing table as the number of hops and path node to the receiver. Similarly, all nodes in the network receive the RCON packet and update their routing tables. Once they are all multiple paths are generated, the node disjoint multipath identified between the source and destination. When the source node to send the data from the target, extends the FFI trace data between nodes disjoint multipath based and long tail filled fill residual energy. If a path disjoint node fails due to the death of routing node movement or node, it informs the source node through the RERR packet.

VII. SIMULATION OF PROPOSED APPROACH

To implement the concept, the aodv.cc file has been modified. When the simulation starts function named “command” is invoked. All the modification related to the wormhole is done in this function. Functionality to create wormhole nodes by reading the node ID from the file is added in this function. The Tcl script calls this function to create wormhole in the simulation. Tcl also calls the attacking and

detecting time, from its related file that is reside in the "command" function.

Parameters	Values	
Number of Nodes	Vary from 40 to 100	
Area	40	600*300
	50	600*300
	100	1000*800
	140	2000*1500
	170	2000*1500
Traffic	CBR	
Simulation Duration	100 Mili Seconds	
Packet Transmission Rate	1024 kbps	
Carrier sense threshold Used In Normal Nodes	200 Meter	

Table 1 Simulation Parameters

Proposed ESAODV show better result in term of packet delivery ratio , battery power consumption and control packet overhead.

Packet delivery ratio:- Proposed ESAODV having higher packet delivery ratio as compare with EENDMRP . EENDMRP has higher degree packet loss.

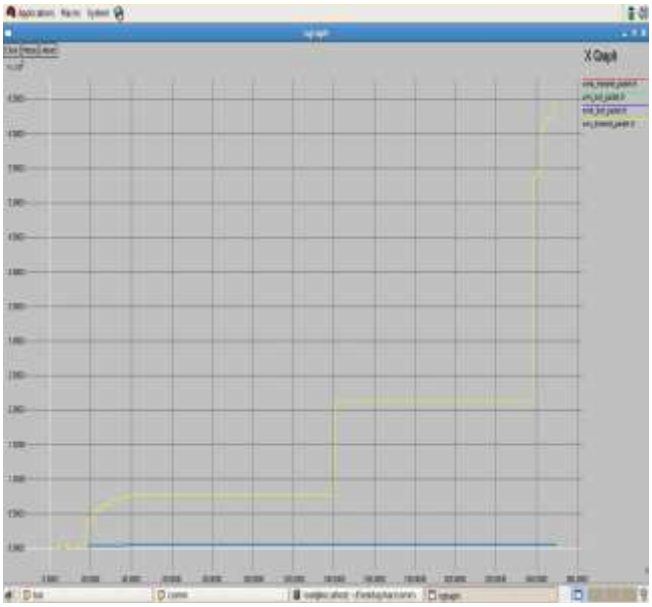

Figure 3 Packet delivery ratio of Proposed Protocol

Control packet overhead:- For any ideal routing protocol it is required that it has lower control packet overhead, whereas existing EENDMRP have required higher control packet as compare to proposed ESAODV.

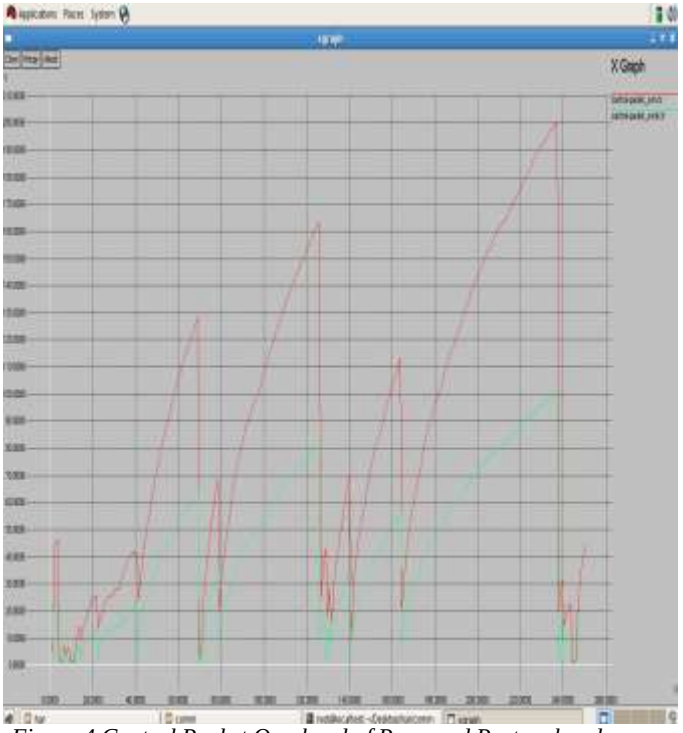

Figure 4 Control Packet Overhead of Proposed Protocol and Existing Protocol

Battery Power Consumption:- Towards Energy saving routing protocol proposed protocol try to move lower energy node towards less traffic and higher energy node towards high traffic and reduce retransmission whereas existing approach only minimized redundant path.

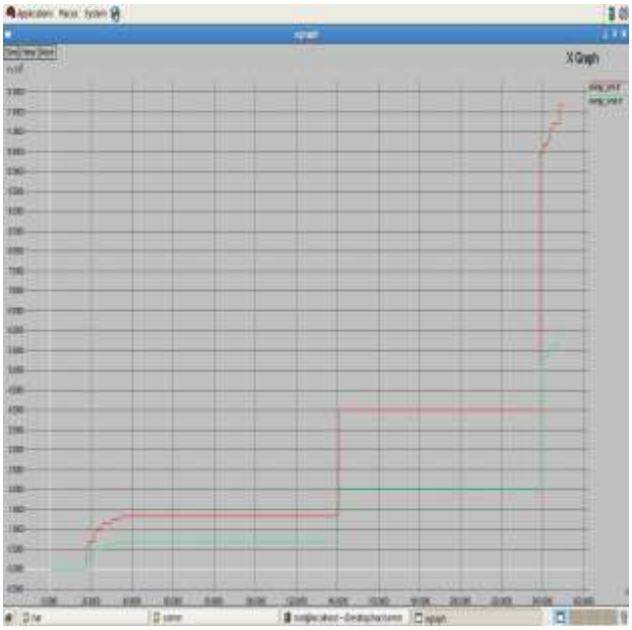

Figure 5 Battery power consumption of Proposed Protocol and Existing Protocol

VIII. CONCLUSION

To improve the reliability through redundant paths in the network, it is suggested to have a maximum number of paths between the source and the destination. It is necessary to have a minimum number of nodes in each redundant path. Network reliability is increased in networks multipath disjoint nodes, where each node disjoint path has a maximum number of redundant paths and the minimum number of nodes in each redundant path. In the multi-path network node disjoint, the reliability is very high.The performance of proposed technique is depending upon network density and network traffic.

REFERENCES

[1] Zunnun Narmawala, Sanjay Srivastava, "Survey of Applications of Network Coding in Wired and Wireless Networks" in Proceedings of the 14th National Conference on Communications, pp. 153-157, February 2008.

[2] Sheikh, R. , Singh Chande, M. and Mishra, D.K., "Security issues in MANET: A review", IEEE 2010, pp 1-4.

[3] Kannhavong, B., Nakayama, H., Nemoto, Y. and Kato, N., " A survey of routing attacks in mobile ad hoc networks" IEEE 2007, pp 85-91.

[4] Verma, M.K. and Joshi, S. ; Doohan, N.V. "A survey on: An analysis of secure routing of volatile nodes in MANET", IEEE 2012, pp 1-3.

[5] Mariannne. A. Azer, "Wormhole Attacks Mitigation in Ad Hoc Networks", IEEE 2011, pp 561-568.

[6] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks In Wireless Networks Using Connectivity Information," in Proc. of IEEE INFOCOM, 2007.

[7] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni and Naghmeh Niknejad, "Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", IEEE 2011, pp 122-128.

[8] Ronggong Song, Peter C. Mason and Ming Li, "Enhancement of Frequency-based Wormhole Attack Detection", IEEE 2011, pp 1139-1145

[9] S. A. Razak, S. M. Furnell and P. J. Brooke, "Attacks against Mobile Ad Hoc Networks Routing Protocols", School of Computing 2004.

[10] Xiangyang Li "Wireless Ad Hoc and Sensor Networks: Theory and Applications" Cambridge University Press 978-0-521-86523-4

[11] Katrin Hoeper, Guang Gong, "Pre-Authentication and Authentication Models in Ad Hoc Networks," Signals and Communication Technology, pp. 65-82, 2007.

[12] H D-Ferriere, M Grossglauser, and M Vetterli, "Age Matters: Efficient Route Discovery in Mobile Ad Hoc Networks Using Encounter Ages," 4th ACM International Symposium on MANET and Computing, 2003

[13] S. Capkun, L. Buttya'n, and J.-P. Hubaux, "Sector: Secure Tracking of Node Encounters in Multi-Hop Wireless Networks" in Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks, 2003.

[14] P. Papadimitratos and Z. J. Haas, "Secure Routing For Mobile Ad Hoc Networks" in Proc. of CNDS, 2002.

[15] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, "A Secure Routing Protocol For Ad Hoc Networks" in Proc. of IEEE ICNP, 2002.