International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com ǁ PP. 69-72

Performance Evaluation of AODV Routing Protocol for Different Node Density and Traffic in Wireless Sensor Networks

Gaurav J.M[1], Keerthi H.K[2], Chithanyaranga H.V[3], Keerthi D.S[4]
[1]*UG student, Department of ECE, Malnad college of engineering Hassan.*
[2]*UG student, Department of ECE, Malnad college of engineering Hassan.*
[3 1]*PG student,Department of ECE, Malnad college of engineering Hassan*
[4]*Asistence professor, Department of ECE, Malnad college of engineering Hassan.*

.

ABSTRACT: The development of the wireless sensor networks (WSNs) in various applications like Defence, Health, Environment monitoring, Industry etc. always attract many researchers in this field. WSN is the network which consists of collection of tiny devices called sensor nodes. Sensor node typically combines wireless radio transmitter-receiver and limited energy, restricted computational processing capacity and communication band width. These sensor node sense some physical phenomenon using different transduces. The current improvement in sensor technology has made possible WSNs that have wide and varied applications. While selecting the right sensor for application a number of characteristics are important. This paper provides the overview of WSNs and the performance of AODV for different node density and traffic is evaluated using Qualnet6.1 simulator from the results AODV performs better for lower node density and traffic as compared to the higher node density and traffic.

KEYWORDS: AODV, Routing Protocols, Sensor node, WSNs.

I. INTRODUCTION

WSNs were primarily introduced for the defence application and the objective here is to on it or activity of enemy without any human interference. A low-flying airplane, ground vehicle or a powerful laptop acted as a base station to collect information from all sensor nodes .WSNs can be presume as a special case of Ad Hoc networks [1]. WSN are generally assumed to be energy restrained because of tiny size sensor node. Even though sensor networks are a subset of Ad Hoc Network, the protocol designed for the Ad Hoc networks cannot be used as it due to the following reason:

a. The number of sensor nodes in a sensor network is very large compared to the Ad Hoc network. Thus sensor networks require distinct and more adaptable solutions.

b. As compared to Ad Hoc network, Wireless sensor nodes have restricted power supply. Andin impractical environment condition they cannot be recharged because the large number of sensor nodes are deployed in different locations[1].

.

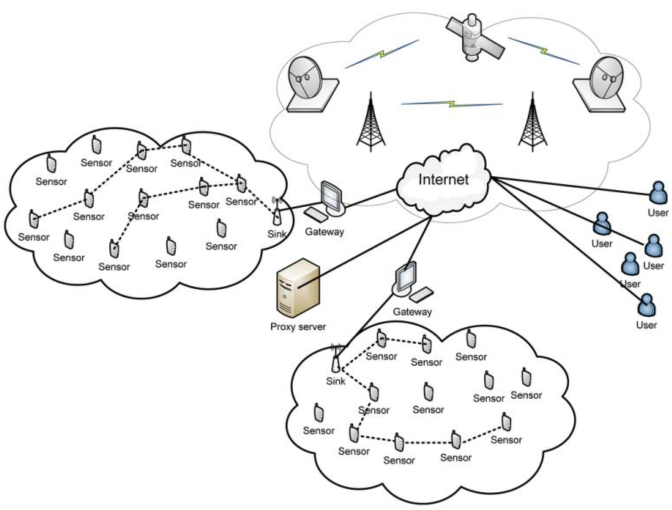


Figure: 1 Wireless Sensor Networks (WSNs)

Thus wireless sensor networks can be defined as "A WSNs consists of spatially distributed autonomous sensor to monitor physical or environmental conditions (i.e. temperature, humidity, pollution, sound, pressure, etc.) and to cooperatively pass their data through the network to user location**"[2]**. The WSNs is built of few to several thousands of sensors of nodes, where each and every node is connected to one or many sensor nodes. Source node is connected to a central gateway, also called as base station. Central gateway provides a connection to world through different communication channels (internet, Wi-Fi, WI-Max, wired LAN etc.). Figure: 1shows data collection from different nodes which further processed and analyzed.

Security: Security is an important issue which implies that both authentication & encryption should be feasible.

II. Routing protocol

AODV: The information in this section concerning the Ad Hoc On Demand Distance Vector Protocol (AODV) protocol is taken from the RFC . AODV is a reactive protocol, i.e., so the routes are created and maintained only when they are needed[4]. The routing table stores the information about the next hop to the destination and a sequence number which is received from the destination and indicating the freshness of the received information[3]. Also the information about the active neighbours is received throughout the discovery of the destination host. When the corresponding route breaks ,then the neighbours can be notified.

The route discovery is used by broadcasting the RREQ message to the neighbours with the requested destination sequence number, which prevents the old information to be replied to the request and also prevents looping problem, which is essential to the traditional distance vector protocols [1]. The route request does not add any new information about the passed- hosts only it increases its hop metric. Each passed host makes update in their own routing table about the requested host. This information helps the destination reply to be easily routed back to the requested host. The route reply use RREP message that can be only generated by the destination host or the hosts who have the information that the destination host is alive and the connection is fresh.[4]

Usually messages are transmitted by using IP limited broadcast address, but the messages are checked for the content so that they will not be broadcasted throughout the entire network. Some of the messages are supposed to be spread widely in the network, for example route request message(RREQ). So their distribution is restricted by the TTL field in the IP header[4]. Usually the fragmentation of the IP packet is not required.

III. Results and Discussion

3.1Performance metrics:

3.1.1 Throughput:

Throughput or network throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over a physical or logical link or it can pass through a certain network node. Throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second (p/s or pps) or data packets per time slot.

3.1.2 Jitter:

Jitter is the deviation from true periodicity of a presumed periodic signal in electronics and telecommunications, often in relation to a reference clock source. Jitter may be observed in characteristics such as the frequency of successive pulses, the signal amplitude, or phase of periodic signals. Jitter is a significant, and usually undesired, factor in the design of almost all communications links.

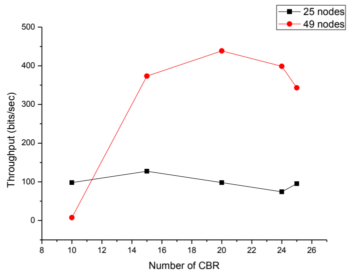
3.1.3 End to end delay:

End-to-end delay or one-way delay (OWD) refers to the time taken for a packet to be transmitted across a network from source to destination. It is a common term in IP network monitoring, and differs from Round-Trip Time.

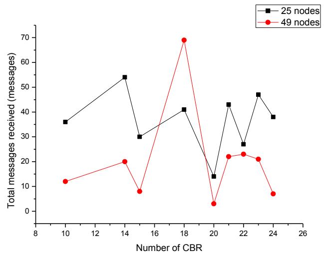
3.1.4 Total message received:

The total messages that are arrived at the receiving node is called the Total message received.

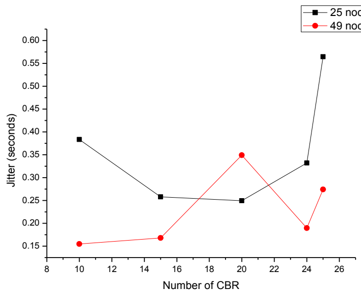
Results:



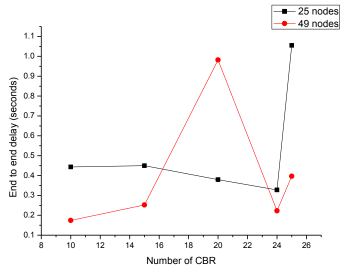
(a)



(b)

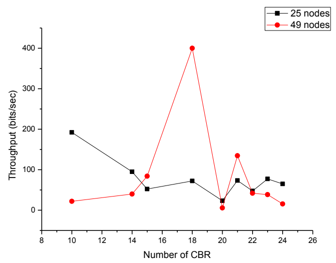


(c)

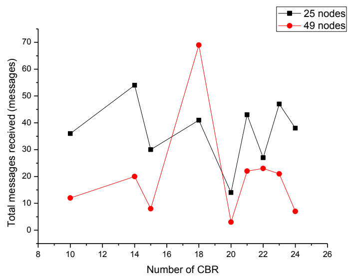


(d)

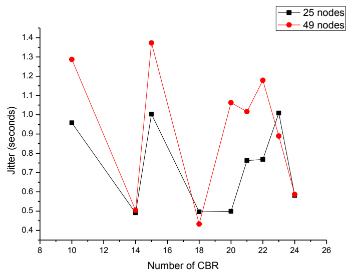
Figure 2: (a) Throughput with 5 CBR,(b)Total messages received with 5 CBR,(c) jitter with 5 CBR (d) end to end delay with 5 CBR



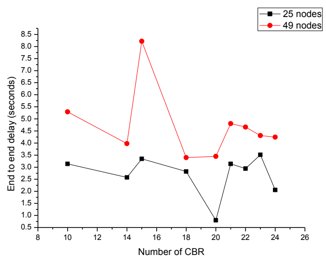
(a)



(b)



(c)



(d)

Figure3 : (a)Throughput with 10 CBR,(b)Total messages received with 10 CBR,(c) end to end delay with 10 CBR, (d) Jitter with 10 CBR .

from the figures 2 and 3 we can observe that the performance of the WSNs is much more efficient when the node densities are less as shown in the figure 2.a the throughput is more in the 25nodes than the 49 nodes and also we can observe that the performance is better in the lesser node density and the lesser traffic systems.

IV. Conclusion and future work:

From the results we can observe that when the node density is less ,the more throughput, less delay ,less jitter and can receive more number of messages received when the node density is high the less throughput, more delay ,more jitter and can receive less number of messages received and also from the number of applications as shown in the figures from figure 2and figure 3 , so that we can conclude that the performance can be more in the lesser node density and lesser applications, in future this can be improved by the modifications of the code

V. Acknowledgement

This work is supported by Tequip-II SPFU Karnataka

VI. REFERENCES

[1]. Joanna Kulik, Hari Balakrishnan and W. R. Heinzelman, (1999) “Adaptive protocols for Information Dissemination in Wireless sensor networks”, proceeding on 5th annual ACM/IEEE International conference on mobile Computing and networking, pp. 174-185.

[2]. ChalermekIntanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann and Fabio Silva, “Directed Diffusion for Wireless Sensor Networking”, IEEE/ACM Transactions on networking (TON), vol. 11, pp. 2-16, February 2003.

[3]. Joanna Kulik, HariBalakrishnan and W. R. Heinzelman, “Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Network,” Wireless Network, vol. 8, pp. 169-185,2002.

[4]. Li Xi Chen and Xiaohong Guan, (2004) “A New Gradient-Based Routing Protocol in Wireless SensorNetworks”, proceedings of the First International Conference on Embedded Software and Systems,pp. 318-325.

[5]. Ankitajoshi and Lakshmi Priya.m, “A survey of Hierarchical Routing Protocols in Wireless Sensor Network”, MES Journal of technology and Management, pp.67-71