ANALYSIS ON AD HOC ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

P.N.Renjith [1] and E.Baburaj [2]

[1] Assistant Professor, Department of Computer Engineering, Lord Jegannath College of Engineering and Technology, Tamil Nadu, India
renjith.ljcet@gmail.com
[2] Professor, Sun College of Engineering and Technology, Erachakulam, Tamil Nadu, India
alanchy_babu@yahoo.co.in

ABSTRACT

Outlook of wireless communication system marked an extreme transform with the invention of Wireless Sensor Networks (WSN). WSN is a promising technology for enabling a variety of applications like environmental monitoring, security and applications that save our lives and assets. In WSN, large numbers of sensor nodes are deployed to sensing and gathering information and forward them to the base station with the help of routing protocol. Routing protocols plays a major role by identifying and maintaining the routes in the network. Competence of sensor networks relay on the strong and effective routing protocol used. In this paper, we present a simulation based performance evaluation of different Ad hoc routing protocols like AODV, DYMO, FSR, LANMAR, RIP and ZRP in Wireless Sensor Networks. Based on the study, the future research areas and key challenges for routing protocol in WSN are to optimize network performance for QoS support and energy conservation.

KEYWORDS

Wireless Sensor Networks, routing protocols, Network topologies

1. INTRODUCTION

Development of Micro Electro Mechanical System favoured a tremendous growth in Wireless Sensor Networks (WSN). Wireless sensor network rapidly become most eminent and promising technology for enabling a variety of applications like environmental monitoring, security, and application that save our lives and assets. WSN consist of low cost, energy constrained and multifunctional wireless sensor nodes which are spatially distributed over any specific geographical area of interest to perform sensing function. Sensor nodes are equipped with sensors which can sense environmental conditions like temperature, humidity, sound, movement, vibrations, pressure and even toxic conditions [1]. WSN encompasses of a substantial number of nodes deployed in a geographical location in which nodes are not directly connected. Hence, the sensed information is passes across with the help of multi-hop communications. Each node senses the information and passes them across to the Master node with the help of multi-hop communication. Cluster head in-turn forwards the aggregated information to the base station. The main aim of data aggregation technique is to collect and aggregate data in an energy efficient manner so that network lifetime is enhanced. Since sensor nodes might generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. This technique has been used to achieve energy efficiency and traffic optimization in a number of routing protocols. Routing protocols are in charge of identifying and maintaining the routes in the network [3].Routing algorithms plays a major role in data transmission from source node to destination. A routing protocol broadcast packets enclosing routing information to nodes deployed in the sensing

DOI : 10.5121/ijasuc.2012.3601

region. It enables the nodes to select a specific route in network. Selection of specific route between source and destination is done by different routing algorithms. A routing protocol share the route information first among immediate neighbours, and then throughout the network. This enables the nodes to understand the network topology of the network. Fig 1.1 explains the working of routing protocol. Initially the source node broadcast 'hello' message to the neighbour node to identify nearest neighbour node. This process of broadcasting hello messages continues until the nodes get aware of the complete network topology.

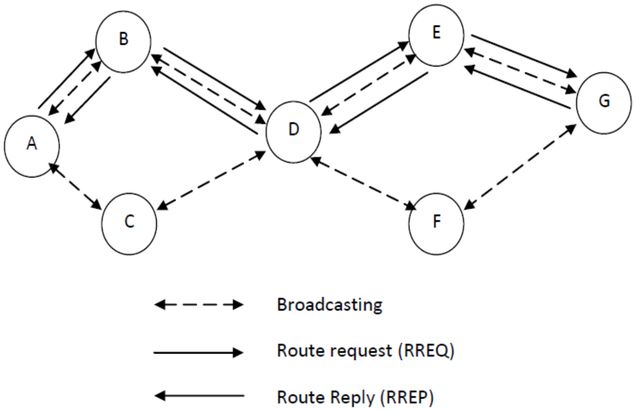

Figure 1. Working of Routing Protocol

Once the topology is identified using the routing algorithm shortest path to the destination is evaluated. The source node sends Route Request (RREQ) to the destination using multi-hop communication. The destination in-turn write back as Route Reply (RREP). It is not mandatory that the destination have to use the same route as the sender node. Destination node can write back by evaluating its own path and send back reply to the source node. Thus source node communicates with the destination. A routing protocol is responsible for determining specific route for communication. The route is evaluated using different criteria like trust worthiness, traffic volume and congestion in the specific path. However, conventional routing protocols have numerous limitations when applied to WSNs, which are mainly due to the power constrained nature of WSN [2]. Major design issue of WSN is that each Sensor nodes are equipped with low powered battery, limited range of sensing, computational, storage and communication resources. Another critical issue while designing routing algorithm for WSN will be unique identification numbering used in conventional routing protocol [3, 4]. In WSN unique number is impossible as number of sensor nodes deployed in a specific region ranges from few hundreds to thousands. Above all, extensive utilization of computational resources and communication resources can potentially reduce the battery life of a Wireless Sensor [5]. Life time of a WSN depends on the Life time of Sensor nodes. After the deployment of sensor devices it is impossible to charge or replace battery. Conventional routing protocols have severe impact when used with energy and computationally constrained Wireless sensor network. Thus, the exceptional uniqueness and constraints of sensor node present made design issue of Routing protocol for WSN is more challenging.

The remainder of this paper is organized as follows. Section 2 of this paper explains Performance characteristics in routing protocol. In Section 3, we introduce different routing protocols like AODV, DYMO, FSR, LANMAR, RIP and ZRP. Simulation setup and parameters are explained in Section 3. A comparative study of routing protocols is discussed in the session 4. Finally, we conclude by describe future research directions in Section 4.

2. PERFORMANCE CHARACTERISTICS OF ROUTING PROTOCOLS

In this session, various performance characteristics are analyzed which may influence the performance of the system with regards to network, users and applications.

2.1. Energy Efficiency

In this session, various performance characteristics are analyzed which may influence the performance of the system with regards to network, users and application.

- Reducing the amount of data transmitted across the network.
- Lower the transceiver duty cycle range.
- Lower the frequency of data transmission.
- Reduce the frame overhead.
- Implementation of strict power management techniques. [9]
- Reduce redundant transmission.
- Reduce computation overhead.

By using a powerful routing protocol, the number of retransmission across the network can be controlled effectively. Typically in a homogeneous or heterogeneous WSN, routing protocol plays a major role by evaluating node density, congestion and network availability [6]. By utilizing effective routing algorithm, network life time and energy will be conserved and redundant transmission will be reduced.

2.2. Average End-to-End Delay

Average End-to-End delay is a metrics used to measure the performance with time take by a pack to travel across a network from a source node to the destination node. In WSN, sensor nodes switch between an active (on) and a sleeping (off) mode, to save energy. Such Scenario pays a greater latency in the sensor network. Each sensor node with sensed data has to wait for the neighbour sensor node to turn it to active mode from sleep mode [10]. End to end delay evaluates latency when data send by sensor nodes and received by destination node. An end to end delay includes all possible delay caused during route discovery, retransmission delay, queuing delay and relay time.

$$\mathbf{D_{end\text{-}end}= N\ (\ D_{trans} + D_{prop} + D_{proc})}$$

Where,

Dend-end	= End-to-End Delay,
Dtrans	= Transmission Delay,
Dprop	= Propagation Delay,
Dproc	= Processing Delay.

2.3. Average Jitter

Average jitter is a performance characteristics used to measure deviation from true periodicity eventually of inactivity in packet across a specific network. When a network is stabilized with constant latency will have no jitter. Packet jitter is expressed as an average of the deviation from the network mean latency [12]. Due to data congestion or route changes can cause jitter. In a Wireless sensor networks, multiple sensor nodes may sense the information and forward them to the sink in continuous manner. Due to bottle neck problem or network congestion in the receiver end a delay may occur. This delay causes a deviation from the jitter. Average Jitter in a network increases indefinitely due to improper queuing techniques or configuration errors.

2.4. Throughput

In a WSN, throughput is measured in terms of successful delivery of data packet within the threshold time. The data may use different routes and passes across multiple intermediate nodes to reach the destination [7]. Throughput is measured using number of bits of packet received per unit time. Normally throughput is measured as bits per sec.

The following are major factors affecting throughput:

- Packet loss due to network congestion
- Available bandwidth
- Number of Users in the Network
- Data loss due to bit errors
- Improper queuing techniques used
- Usage of Weighted Fair queue or priority queue
- Slow Start and multiple decrease techniques

2.5. Network Lifetime

Lifetime of the WSN depends on the life of the sensor nodes [1]. In WSN, sensor nodes have data to send to a base station. It is more essential to reduce the total energy consumed by the system to maximize the network lifetime of the network. With the implementation of effective routing protocol, power consumption per node can be balanced; network lifetime can be significantly increased [13]. Network Lifetime of WSN can be derived from the formula (1) [14].

$$\mathbf{E[L]} = \frac{(\,\boldsymbol{\varepsilon}\mathbf{0} - \mathbf{E[E\omega]})}{(\mathbf{Pc} + \boldsymbol{\lambda}\,\mathbf{E[Er\,]})} \quad \ldots\ldots\ldots\ldots\ldots\ldots.. \quad (\mathbf{1})$$

ε0 - initial non rechargeable energy
E[L]-average network lifetime
Pc- constant continuous power consumption
E [Eω] -expected wasted energy
λ- Average sensor reporting rate
E[Er] -Expected reporting energy consumed [21].

2.6. Scalability

Scalability in WSN is the ability of a network to handle maximum sensor node deployed a specific area. A WSN consists of hundreds to thousands of sensor nodes. Routing protocols must be workable with this huge number of nodes i.e., these protocols can be able to handle all of the functionalities of the sensor nodes so that the network lifetime can be stable. Scalability results in complete topological changes. Deployment of sensor nodes can be either manual or random deployment. When a sensor node is deployed manually, routing protocol can be able to determine the node identity so proactive routing protocol will be much helpful. However, in random deployment, determining node using unique identification number is very difficult. Hence reactive type of routing protocol will be helpful in evaluating random deployment. Node deployment in a specific geographical area can be limited by evaluating the maximum scalability of sensor node in the specific region based on area and radio transmission range. For example, it can refer to the capability of a network to increase total throughput under an increased sensor in any particular area are added [1].

Scalability can be measured using the density formula

$$\boldsymbol{\mu(A)} = \frac{\boldsymbol{N\pi R^2}}{\mathbf{A}} \ldots\ldots..\ldots\ldots\ldots\ldots.. \quad \mathbf{(2)}$$

Where R is the Radio Transmission Range

A is the area of the specific Sensor region.

2.7. Packet Delivery Ratio

Packet delivery ratio is a performance metrics used to evaluate total packets properly delivered. It is the ratio of total amount of data packets received at the destination to total packet transmitted at the source. To evaluate the packet delivery ratio, the packet send from the source and the packet received at the destination should be recorded. Source node transmits the information to destination with sequenced packet with sequence number. If a packet fails to reach the destination either by discard or by congestion control mechanism, the source node retransmit the packet based on retransmission timer algorithm. However, number of retransmission increase the transmission overhead and cause very low packet delivery ratio. When number of source and destination increases the transmission complexity also increases. It is the duty of a routing protocol to manage packet routing with shortest and reliable path. Packet delivery ratio is calculated by dividing the number of packet received by destination through the number packet originated from source [9].

$$\text{Packet Delivery Ratio } (PDR) = \frac{\text{Packet received at the Destination}}{\text{Packet transmited by the source}}$$

3. OVERVIEW OF ROUTING PROTOCOLS

Routing protocols are specific algorithm designed to perform the way the routing within sensing region. A routing protocol shares the route information primarily with first-hop neighbours, and then spreads the route information throughout network. This time period can be called as learning time in the network; by this process all sensor nodes gain knowledge of the entire topology of the network. In this session, different routing protocols like AODV, DYMO, FSR, LANMAR, RIP and ZRP are discussed.

3.1. Ad hoc On Demand Distance Vector (AODV)

Ad hoc On Demand Distance Vector (AODV) Routing Protocol uses on demand approach to discover and identify a specific route. When a node requires sending data, AODV uses route discovery using control messages like route request (RREQ) and route reply (RREP) to find the route to destination. In AODV protocol neighbour nodes stores the route information of its next hop neighbour. This enables AODV to evaluate the shortest distance and safe path. To discover a path source node broadcast a route request message to its immediate neighbour. Neighbour in-turn sends the route request packet to its neighbour. This process continues until the destination is reached. When the Route Request (RREQ) packet reaches the destination, destination node writes back with Route Reply (RREP) and window size for data transmission. Once the data packet is transmitted the route information will be cleared. AODV protocol discovers and identify route only when nodes require sending or receiving data. During error while transmission or link failure a route error (RERR) message will be generated and send it to the source node to find alternative path. The main advantage of AODV protocol is route is discovered and identified on demand. AODV faces severe drawback as intermediate nodes may forward to unreliable routes if the source sequence number is very old and the intermediate nodes have a higher, but not the related to latest destination sequence number [10].

3.2. Dynamic MANET On-demand (DYMO)

The Dynamic MANET On-demand (DYMO) routing protocol enables reactive, multi-hop unicast routing technique. Main operation of DYMO is to perform route detection and route preservation. During route detection, the sender node initiate route request throughout the network to identify the destination node in the network. Destination node in-turn writes back to the source with route reply (RREP). However, destination node may also use different route to reach the source node. It is not mandatory for the source and destination to use same path for communication. Route request and Route reply are passed across the network by unicast hop-by-hop communication. In DYMO, route maintenance is performed as 2 operations. To protect the existing routes, DYMO routers lifetime is increased with every successful delivery of packet. In order to identify the changing network topologies, DYMO routes will be monitoring entire network links through which network traffic is forward. When a packet reaches any node by forwarding and node have no information of destination, then the node informs the Source node with route error (RERR). A Route Error (RERR) is an error packet send to the source or destination to notify that the path or link is invalid or missing [22].

3.3. Fisheye State Routing Protocol (FSR)

Fish eye is a proactive and hierarchical routing protocol. FSR uses the technique followed by a fish eye. Fish eye normally observers and focus with high detail on the object very close to its focal point. When the object distance increases from the focal point the detail decreases. The same principle is used in Fisheye State routing. FSR maintain topology map at each node.FSR will not flood or broadcast to evaluate the route. Instead, nodes maintain a link state table based on updated information from the neighbour. A full topology map will be stored in each node of the network. The topological map will be utilized to route discover and route maintenance. Shortest path will also be evaluated using topological map [22].

3.4. LANMAR Routing Protocol

LANMAR is an effective proactive based routing protocol which uses the same approach of Fisheye State Routing (FSR).Routing table and Node distance is evaluated using hop counts in the given network topology. LANMAR stores a specific address each node reflects its position within the hierarchy and enables LANMAR to discover and maintain a specific route [23]. All the nodes in a specific hierarchy region gain knowledge of route to communicate with each other. Moreover, each node will be defined with a specific “landmarks” at different hierarchical levels. In LANMAR routing protocol there is consistent packet forwarding and the path is redefined from top level hierarchy to lower level hierarchy. When a node requires sending a packet within its hierarchical region, the route information is identified from the routing table stored within the hierarchical region. Otherwise, node evaluates the logical subnet field of the destination and the packet is forwarded towards the landmark for that consistent subnet. Topological changes and route information will be updated periodically within the hierarchical nodes with one hop distance. In every update, the nodes will send the route information based on its fisheye scope. By this updating process, the routing entries with larger sequence numbers are replaced with smaller sequence numbers [23].

3.5. Zone Routing Protocol (ZRP)

The zone routing protocol is a combination of reactive and proactive routing protocol. ZRP takes the advantages of both reactive and proactive routing protocols. Major drawback of Proactive routing protocol is excess bandwidth is utilized while maintain a routing information. However, in reactive routing protocol initiates unwanted delay in the network by increasing route request and route reply wait time. Reactive routing protocol causes major energy conception by broadcast route request and route reply. The Zone routing protocol admits these problem network delay and excess energy utilization. In Ad-Hoc network if network congestion is most likely to occur, the path will be changed or packets will be diverted to nearby node. In ZRP route information is maintained only with sensor nodes which stay on the routing zone. In ZRP A sensor node discovers and identify its zone through a proactive scheme called Intra zone Routing Protocol (IARP). For nodes outside the routing zone, Inter zone Routing Protocol (IERP) is responsible for reactively discovering routes to destinations. The major difference of IERP is identifying and maintain a route record of nodes exist in the Routing Zone. This will reduces the unnecessary broadcast of route request to identify the nearest neighbour.

4. Simulation Setup

QualNet 5.2 Network Simulator tool is used to evaluate the performance of different Ad hoc routing in Wireless sensor networks. In this simulation, we have tested routing protocols with 10, 25, 50, 100, 200, 250 nodes. The nodes are deployed randomly in a terrain of 200 X 200 m^2. CBR is used as data traffic application with multiple source and destination. The parameters used in the simulation are summarized in the table below:

Table 1. Parameters used in the Simulation

Parameters	Values
Routing Protocols	AODV, DYMO, FSR, LANMAR, RIP, ZRP
MAC Layer	802.11
Packet Size	512 bytes
Terrain Size	200 X 200 m^2
Nodes	10, 25,50, 100, 200, 250
Node placement	Random
Data Traffic Type	CBR
Source	Multiple source and Destination
Total bytes of data sent	12888 bytes
Simulation Time	3000 sec
Antenna Type	Omni Directional
Simulator	QualNet 5.2

5. Comparative Study on Routing Protocols

In table 2 comparative study of different routing is made based on performance characteristics in wireless sensor networks. Performance metrics like throughput, average Jitter, End-to-End Delay, packet delivery ratio are compared with variable node density like 10, 25, 50, 100, 200 and 250. Performance analysis is made using QualNet 5.2 on AODV, DYMO, FSR, LANMAR, RIP and ZRP routing protocols. In the wireless Sensor Networks have most challenging task is life time. Competence of sensor networks relay on the effective routing protocol used.

Table 2. Comparative Study on different routing protocols

Number of Nodes	Routing Protocol	Average Jitter (s)	Average End-to-End Delay (s)	Throughput (bits/s)	Packet Delivery Ratio	Last Packet Received at (s)
10 Nodes	AODV	0.00323	0.003619	4275	1	24.0036
	DYMO	0.004186	0.003693	4275	1	24.0036
	FSR	0.000211	0.003406	4291	0.916667	24.0036
	LANMAR	0.000159	0.003389	4274	1	24.0032
	RIP	0.00018	0.003388	4274	1	24.0033
	ZRP	0.00022	0.003445	4274	1	24.0036
25 Nodes	AODV	0.008068	0.008906	4275.25	1	24.0084
	DYMO	0.006951	0.008815	4275	1	24.0084
	FSR	0.017061	0.016895	4271	1	24.0225
	LANMAR	0.003999	0.008477	4273	1	24.0092
	RIP	0.003877	0.008427	4273.75	1	24.0082
	ZRP	0.005012	0.008528	4273.5	1	24.0084
50 Nodes	AODV	0.022882	0.020842	4278.89	1	24.0205
	DYMO	0.05657	0.021537	4291.11	1	24.018
	FSR	0.489806	0.464972	4138.56	0.972221	24.7893
	LANMAR	0.068934	0.107234	4273.78	1	24.0171
	RIP	0.01196	0.017634	4273.22	1	24.0181
	ZRP	0.015837	0.020927	4273.89	1	24.0168
100 Nodes	AODV	0.011441	0.014371	4275.57	1	24.0152
	DYMO	0.115979	0.023874	4315.57	1	24.0172
	FSR	0.902608	0.839571	694.4	0.2	7.26355
	LANMAR	0.1338	0.358421	731.571	0.208333	7.93772
	RIP	0.009511	0.0179	4280.43	0.964288	24.0162
	ZRP	0.017406	0.023798	4274	1	24.0133
200 Nodes	AODV	0.018226	0.018354	4278	1	24.0185
	DYMO	0.01602	0.01785	4277.11	1	24.0172
	FSR	0.037252	0.165054	289	0.083333	3.94987
	LANMAR	0.06532	0.048659	1174.4	0.075	9.03324
	RIP	0.017891	0.017382	4291.6	0.941667	24.014
	ZRP	0.041416	0.048568	4273.56	1	24.0205
250 Nodes	AODV	0.009539	0.012615	4275.67	1.000488	24.0117
	DYMO	0.132947	0.023775	4324	1.000521	24.0125
	FSR	0.143212	0.076316	152	0.12818	3.07632
	LANMAR	0.151331	0.116372	435.5	0.167046	4.0091
	RIP	0.064483	0.024777	4319.75	1.000783	24.0188
	ZRP	0.029223	0.033656	4273.67	1.000529	24.0127

5.1 Average Jitter

Average jitter is a performance characteristics used to measure deviation from true periodicity eventually of inactivity in packet across a specific network. Performance of different routing protocol based on average jitter is explained in the Figure 2 for node densities10, 25, 50, 100, 200 and 250 nodes. The average Jitter result shows that AODV protocol outperforms all other protocols. FSR protocol shows higher jitter while other protocols average Jitter values were not stable as AODV protocol.

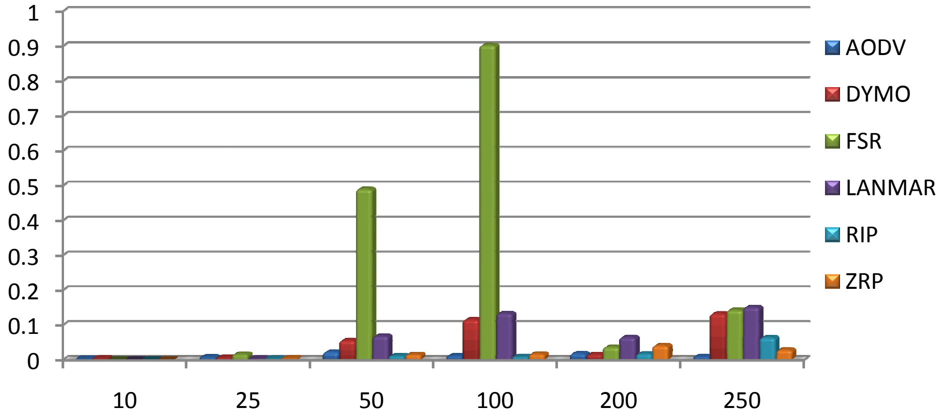

Figure 2. Average jitter vs. Number of Nodes

5.2 Average End-to-End Delay

Average End-to-End is performance metrics used to measure the time take by a pack to travel across a network from a source node to the destination node. Figure 3 explains performance of different routing protocol with different node densities. While examining end to end delay routing protocols were performing more or less equal when node density was less than 50. When node deployment number increased few protocol shows drastic variation. While comparing results with different node densities FSR, LANMAR faces heavy delay. AODV, DYMO and RIP perform better in varying situations.

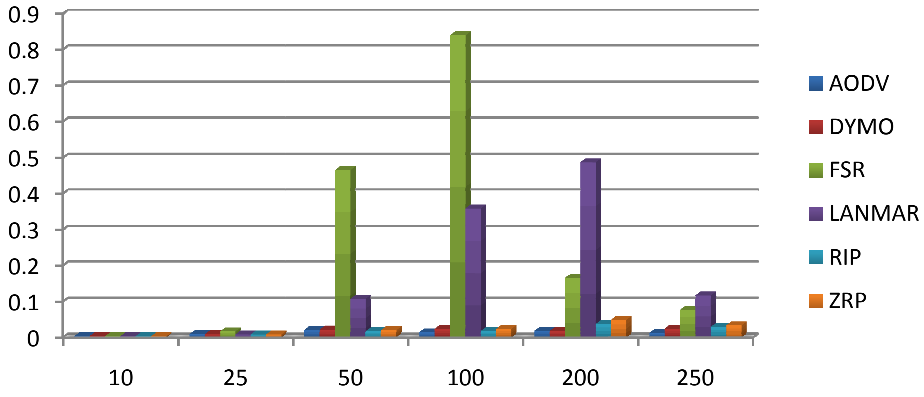

Figure 3. Average End-to-End delay vs. Number of Nodes

5.3 Throughput

Throughput is measured in terms of successful delivery of data packet within the threshold time. Figure 4 explains Throughput of different routing protocols with variable node density. Initially with lesser number of nodes all the routing protocols showed a better result. However, with increase of node density FSR, LANMAR faced a severe delay. AODV, DYMO and ZRP's performance was stable.

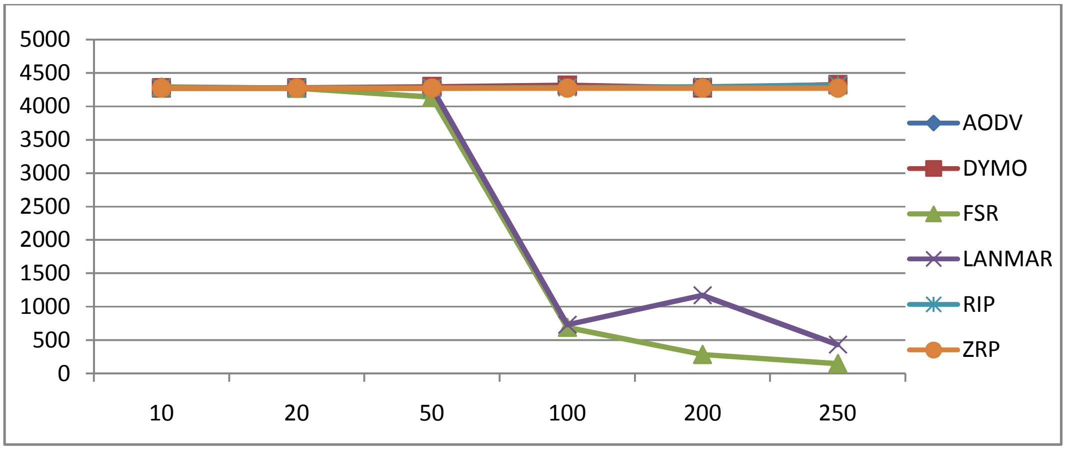

Figure 4. Throughput vs. Number of Nodes

5.4 Packet Delivery Ratio

Packet delivery ratio helps to evaluate total packets properly delivered. It is the ratio of total amount of data packets received at the destination to total packet transmitted at the source. Figure 5 explains graphical representation of packet delivery ratio of different routing protocol with varying number of sensor nodes. The results were similar as previous experiments. When sensor node count was lesser all routing protocol are equally proficient. However, when node deployment count increased most of the protocols were ailing. FSR, LANMAR and RIP faces very low packet delivery ratio. AODV, DYMO and ZRP outperforms while evaluating packet delivery ratio.

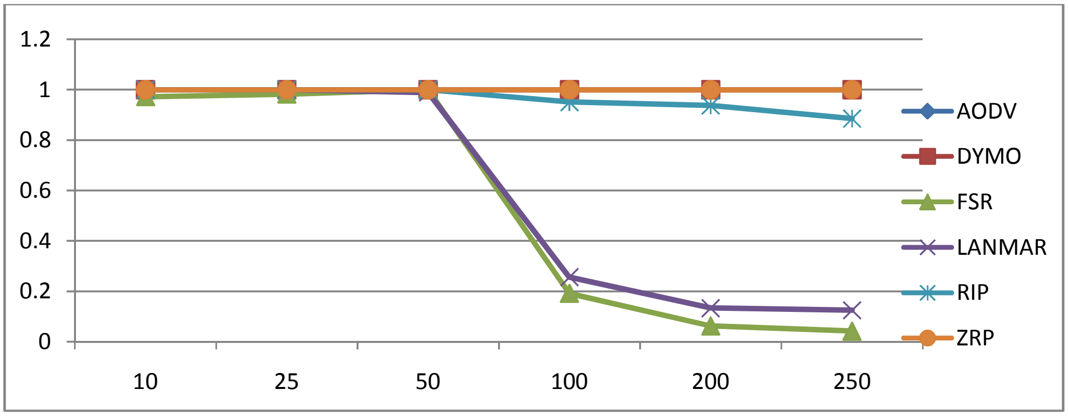

Figure 5 Packet Delivery ratio vs. Number of Nodes

5.5 Evaluation of Routing Protocols

Based on the study and from figure 2, figure 3, figure 4 and figure 5 we obtain conclusion that AODV, DYMO performs better than FSR, LANMAR and RIP. Even in case of lower node density and higher node density AODV and DYMO was able to perform much effectively when compared with FSR, LANMAR and RIP routing protocol. FSR faces heavy challenges when node density is increased. RIP performs better with the calculation of average jitter. However, RIP failed to prove its consistence in throughput and end-to-end delay. It is also noticed that Sensor network is an application based network therefore we can't conclude by saying any routing protocol is outperforming the other protocols.

6. RESEARCH DIRECTIONS

Based on the study on different routing protocols with various performance characteristics, the future research area and issues are explained in this session. The design of routing protocols in WSNs is inclined by numerous challenging factors. These factors must be overcome to achieve efficient communication in WSNs. Due to the condensed computing, broadcasting and battery resources of sensors, routing protocols in wireless sensor networks are expected to achieve the following requirements.

6.1 Node Deployment

Performance of WSN is influenced by node deployment. Sensor nodes can be deployed manually or random manner. When sensors are manually placed and data is routed through pre-programmed paths. However, when the nodes are randomly deployed, the sensor nodes are sprinkled arbitrarily creating a communications in an Ad hoc mode. Unique identification of each sensor is practically impossible as hundreds or thousands of nodes will be deployed at interested geographical area. Sensor nodes are even deployed underwater and under soil. An effective research work should be carried out on node deployment and identification of active nodes in the given specific geographical area. Routing algorithm should support and flexible with changing environmental conditions.

6.2 Energy Consumption

Wireless sensor networks are energy constrained network. One of the major design issues in WSN is preservation of the energy accessible at each sensor node. In any case, energy is a very critical resource and must be used very sparingly. Sensor nodes have to limit the transmission and computation to prevent ultimate utilization of energy resource. In such scenario, routing algorithm has to be designed to reduce packet broadcast during learning curve and to update the route.

6.3 Data Reporting Model

An effective routing protocol has to be implemented to perform faster and efficient data reporting. Sensed data should be reported immediately to the Master node. Queried request will be send from the base station to the sink to evaluate and find the appropriate result. Queries are formulated based on the time interval and intensity of the sensing information. Based on the interval and intensity of available resource the base station will be able to formulate the query. Effective query driven routing protocol will be helpful to fetching right information or time driven approach can be implemented for continuous monitoring. Application like Temperature and humidity monitoring queries will be executed periodically. In such case queries should be formulated to perform periodical sensing. Hence, a routing protocol should be designed which can perform an efficient reporting.

6.4 Security

The security issues with sensor nodes have become most prominent field of research studies. Security has become of supreme consequence with sensor networks being deployed in serious deployment areas like military, aviation and in medical field. However, implementation of security on WSN has greater impact on QoS. A serious work have to be carried out on different types of threats in sensor networks like Spoofing, eavesdropping and most vulnerable attacks like altering routing information, sinkhole attacks, DoS attacks and Jamming attack.

7. CONCLUSIONS

Wireless sensor networks have emerged as a promising technique that revolutionizes the way of sensing information. It has extensive ranges of challenges like Security, topological changes and higher scalability still required to be addressed. In this paper we have presented an analysis on performance evaluation of AODV, DYMO, FSR, LANMAR, RIP and ZRP routing protocols for CBR data traffic type are with varying the node density (25, 50, 100, 200 and 250) using Qualnet 5.2. This analysis helped us to spot a wide-range of issues related with routing in WSN. The routing protocols have to be effectively enhanced or new protocols have to be deployed to resolve the challenges like dynamic topology changes and increased scalability. Future perspectives of this work are focused towards modifying one of the above routing protocols such that the modified protocol could cope with dynamic topological changes and higher scalability with energy efficient routing for the entire Sensor Network.

REFERENCES

[1] I. Akyldiz, W.Su, Y. Sankarasubramanian and E. Cayirci, “A survey on sensor networks,” IEEE Communication Mag., vol. 40, no. 8, Aug. 2002, pp. 102-14.

[2] C. Shen, C. Srisathapornphat, and C. Jaikaeo, “Sensor information networking architecture and applications,” IEEE Personnel Communications, Aug. 2001, pp.52-59

[3] Luis Javier GarcíaVillalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and CláudiaJacyBarenco Abbas "Routing Protocols in Wireless Sensor Networks" Sensors 2009,9,8399-8421;doi:10.3390/s91108399.

[4] Chien-Ming Chen, Yue-Hsun Lin, Ya-Ching Lin, and Hung-Min Sun, “RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks” IEEE Transactions on parallel and distributed systems, vol. 23, no. 4, april 2012.

[5] S. Tilak, N. Abhu-Gazhaleh, W. R. Heinzelman, “A taxanomy of wireless micro-sensor network models,” ACM SIGMOBILE Mobile Comp. Commun. Rev. , vol. 6, no. 2, Apr. 2002, pp. 28-36.

[6] S.W. Arms, C.P. Townsend, D.L. Churchill, J.H. Galbreath, S.W. Mundell , “Power Management for Energy Harvesting Wireless Sensors ” SPIE Int’l Symposium on Smart Structures & Smart Materials.

[7] S.S. Pradhan, K. Ramchandran, “Distributed Source Coding: Symmetric rates and applications to sensor networks”, in proceeding of the data compressions conference 2000, pp.363-372.

[8] JyotirmoyKarjee, H.S Jamadagni, “Data Accuracy Estimation for Spatially Correlated Data in Wireless Sensor Networks under Distributed Clustering”

[9] Olivier Dousse, PetteriMannersalo, Patrick Thiran “Latency of Wireless Sensor Networks with Uncoordinated Power Saving Mechanisms” MobiHoc’04, May 24–26, 2004, Roppongi, Japan.

[10] C.Perkins, E.B.Royer and S.Das,”AdHoc On-Demand Distance Vector (AODV) Routing”, RFC 3561, IETF Network Working Group, July 2003”

[11] Guangya Pei, Mario Gerla and Tsu-Wei Chen "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks" IEEE Communications Letters, 2000

[12] Guangyu Pei, Mario Gerla and Xiaoyan Hong "LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility" http://nrlweb.cs.ucla.edu/ publication/download/199/mobihoc00.pdf

[13] HuseyinOzgur Tan and Ibrahim Korpeoglu, “Power Efficient Data Gathering and Aggregation in Wireless Sensor Networks”

[14] Yunxia Chen, Student Member, IEEE, and Qing Zhao, Member, IEEE “On the Lifetime of Wireless Sensor Networks” IEEE Communications Letters, VOL. 9, NO. 11, November 2005.

[15] Malkin, Gary Scott (2000). RIP: An Intra-Domain Routing Protocol. Addison-Wesley Longman. ISBN 0-201-43320-6.

[16] Xerox System Integration Standard - Internet Transport Protocols (Xerox, Stamford, 1981)

[17] NoritakaShigei, Hiromi Miyajima, Hiroki Morishita, Michiharu Maeda “Centralized and Distributed Clustering Methods for Energy Efficient Wireless Sensor Networks”Proceedings of the International MultiConference of Engineers and Computer Scientists 2009 Vol I IMECS 2009, March 18 - 20, 2009, Hong Kong.

[18] A Heinzelman, W.; Chandrakasan, A.; Balakrishnan, H. Energy–efficient communication protocol for wireless microsensor networks. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences(HICSS), Big Island, HI, USA, January 2000; pp. 3005-3014.

[19] Manjeswar, A.; Agrawal, D.P. TEEN: A protocol for enhanced efficiency in wireless sensor networks. In Proceedings of 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, USA, 2001; p. 189.

[20] Martorosyan, A.; Boukerche, A.; NelemPazzi, R.W. A taxonomy of cluster-based routingprotocols for wireless sensor networks. In International Symposium on Parallel Architectures, Algorithms, and Networks, Sydney, NSW, Australia, May 7–9, 2008; pp. 247-253.

[21] Haowen Chan, Adrian Perrig. "Efficient Security Primitives from a Secure Aggregation Algorithm.” In Proceedings of the Proceedings of the ACM Conference on Computer and Communications Security (CCS)2008.

[22] sitirahayuabdul aziz1, nor adora endut2, shapinaabdullah "performance evaluation of AODV,DSR and DYMO routing protocol in MANET" conference on scientific& social research CSSR0814 - 15 march 2009.

[23] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen, “Scalable Routing Strategies for Ad-hoc Wireless Networks,” In IEEE Journal on Selected Areas in Communications, Aug. 1999, pp. 1369-1379.

[24] Jamal, N.; E. Kamal, A.-K.A. Routing techniques in wireless sensor networks: A survey. IEEE Wirel. Commun. 2004, 11, 6-28.

[25] Braginsky, D.; Estrin, D. Rumor routing algorithm for sensor networks. In Proceedings of theFirst Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, USA, October 2002.

[26] Akkaya, K.; Younis, M. A survey on routing protocols for wireless sensor networks. J. Ad HocNetw. 2005, 3, 325-349.