ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

COMPARISON OF ROUTING PROTOCOLS USED IN WIRELESS SENSOR NETWORKS

Sonika*, Munish Dhar
* Assistant Professor, ECE, Doaba Khalsa Trust Group of Institutions, Rahon, SBS Nagar, INDIA
Assistant Professor, ECE, Doaba Institute of Engineering & Technology, Kharar, Mohali, INDIA

ABSTRACT

Wireless Sensor Networks are used in number of applications due to technological advancements. As WSNs are made up of tiny sensor nodes and moreover these nodes are battery operated devices, so it became very easy to deploy networks based on wireless sensors. As requirement for establishment and effectual working of every type of network are different, same is the case with WSNs. The set of rules which helps in communication of any type of network is known as Protocol, the selection of protocol is an important issue. As WSNs are new and very advanced in features, it became necessary to choose efficient protocol for establishing network based on wireless sensors. In this paper, we are going to analyze protocols used in WSNs & analysis is performed on the basis of comparison of different parameters.

KEYWORDS: WSN, PROTOCOL, AODV, DSR, DSDV, ZRP.

INTRODUCTION

Wireless Sensor Networks has become a cosmic area of research due to its prospective to enable applications that binds physical world to the virtual world. Due to the use of small sensing nodes, it is very easy to establish networks anywhere. Sensor Networks possesses distinctive properties which are not there in traditional networks [1]. Architecture is the vertebrae of any network [2]. So, it became important to discuss briefly the architecture of WSN. From architectural point of view, the WSNs consist of nodes for data gathering [3]. The sensing nodes collect the information from the deployed environment, process and compress it and then transmit it to the base station for further proceedings [3]. These nodes are self organized and work in spontaneous manner [4]. Most of the sensor networks are installed in intimidating environments with active intelligent opposition hence security is a critical issue [5]. Architecture of WSN is represented in Fig. 1.1. A typical WSN consists of the following components:

- Sensor Nodes (Field Devices)
- Gateway
- Network Manager
- Security Manager

WSNs can collect information from those places where conventional networks can't do anything. The applications include home security, military operations, health monitoring, environment monitoring [6] etc. In military operations the main concern is of security and in case of environment monitoring, correct figures are required to predict the status of environment. So, it is clear that every application require different type of protocol which is efficient, reliable and most important secure. Traditional network protocols are not applicable for wireless networks because the medium of communication is different. Traditional networks are based on fixed architecture & topology whereas sensor networks do not follow any fixed structure as well as don't follow any particular topology. Therefore, the rules which are used for traditional networks they are not applicable on wireless networks.

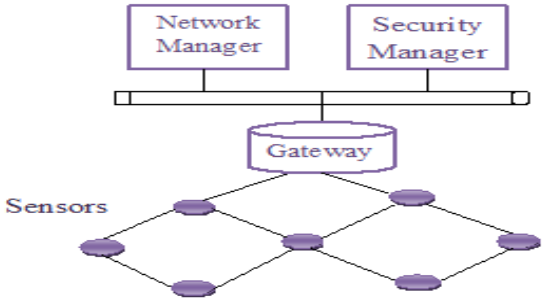

Figure 1: Architecture of WSN

This paper is organized in five sections: Section I includes Introduction, Section II includes comparison of MANETS & Sensor Networks, Section III includes classification of protocols in detail, Section IV is of comparison of protocols and Section V is of conclusion of the analysis.

COMPARISON OF SENSOR NETWORKS & MANETS

Table 1: Comparison of WSN and MANETs

PARAMETER	WSN	MANET
Scalability	Huge amount of sensor nodes	Significantly less number of nodes
Energy	No recharge or replacement of batteries	Energy constrained but energy can be recharged
Self configurability	Almost equal to MANETs but different data traffic and energy trade-off's	It is one of the main feature in MANETs
Environment Interaction	A lot of environmental interactions	More conventional human driven applications with well understood traffic characteristics
Mobility	Mostly stationary use but movement for certain applications possible	One of the main feature of MANETs is that they are caused by moving nodes.
Data Centric	Redundant deployment makes data centric protocols attractive	Data centric protocols are more or less irrelevant for MANETs
Application Specific	Infinite number of applications in terms of devices, protocols, density etc.	Although a few scenarios not as many as in WSN's

MANETS & Sensor networks are two special classes of wireless Ad-Hoc networks. Both networks (WSNs & MANETS) shares some characteristics those are same. On the other hand they are also very different from each other. Although both of them are the types of wireless Ad-Hoc networks but they are of different perspectives. Sensor networks are mainly deployed in geographical areas for tracking & monitoring applications whereas MANETS are established to operate in alliance. Both WSNs and MANETs have many similarities as well as a number of differences. Wireless sensor networks resembles with a mobile ad hoc network because firstly both are distributed wireless networks and are self configurable which consists of nodes connected by wireless links. Secondly, both are usually battery powered and therefore there is a big concern on minimizing power consumption. In both there are limited resources and, traditional protocols and networking algorithms are inadequate [7].
The major differences between MANETS & Sensor networks are discussed in table1

CLASSIFICATION OF PROTOCOLS

Taking into account the reduced capabilities of sensors, the communication with the sink could be initially conceived without a routing protocol. In this premises, the flooding algorithm is used as the simplest solution. In this algorithm, the transmitter broadcasts the data which are consecutively retransmitted in order to make them arrive at the intended destination. Although it is simple but has significant drawbacks. Firstly, an implosion is detected because nodes redundantly receive multiple copies of the same data message. Then, as the event may be detected by several nodes in the affected area, multiple data messages containing similar information are introduced into the network [8]. One solution to this is the gossiping algorithm. In gossiping algorithm the node transmits the message to a selected neighbor node instead of informing all its neighbors as in the classical flooding algorithm, thus avoids implosion. However, overlap and resource blindness are still present. These inconveniences are increased when the number of nodes in the network increases. Thus due to the deficiencies of the previous strategies, routing protocols become necessary in wireless sensor networks One of the main limitations is the identification of nodes. Since wireless sensor networks are formed by a significant number of nodes, the manual assignation of unique identifiers becomes infeasible [11]. The use of potentially unique identifier such as the MAC (Medium Access Control) address is not recommended as it forces a significant payload in the messages [9]. However, this drawback is easily overcome in wireless sensor networks since an IP address is not required to identify the destination node of a specific packet. In fact, attribute-based addressing fits better with the specificities of wireless sensor networks. In this case, an attribute such as node location and sensor type is used to identify the final destination. Once nodes are identified, routing protocols are in charge of constructing and maintaining routes between distant nodes. The different ways in which routing protocols operate make them appropriate for certain applications [10].

All the routing protocols are categorized under three categories: Table Driven (proactive), Source Initiated (reactive) and Hybrid [8].

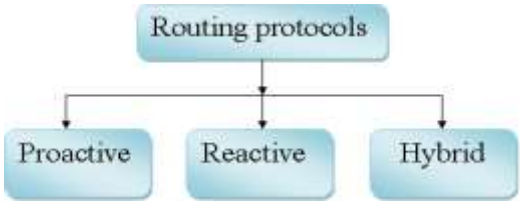

Figure 2 : Routing Protocols

Table-Driven (Proactive Protocols)

- Traditional distributed shortest-path protocols
- Maintain routes between every host pair at all times
- Based on periodic updates; High routing overhead
- Example: DSDV (destination sequenced distance vector)

DSDV is a table driven/proactive routing protocol for ad-hoc networks and is based upon Bellman-Ford algorithm a specified by RIP [12]. This solves the routing loop problem experienced in link state and distance vector routing protocols. DSDV adds, sequence number, a new attribute in each new entry of the routing table. Using this new attribute, stale route information can be distinguished from new one by the mobile nodes and the problem of loop formation can be avoided [13]. Every node maintains a monotonically increasing sequence number for itself [8].In

this proactive protocol routes to all nodes are already discovered in advance and whole table is broadcasts after a fixed interval of time independent of any route changes or not. Data broadcasted by each node contains destination address, number of hopes required to reach the destination, sequence number of information received w.r.t destination. If a link is present sequence numbers will be even otherwise an odd number is used. This number is generated by the destination and the sender makes use of this number to transmit the next new update. The updates can be send as "full dump" which sends full routing table to the neighboring nodes & make use of large number of packets or "incremental update" which send only those entries which results in any change & use less packets [14].

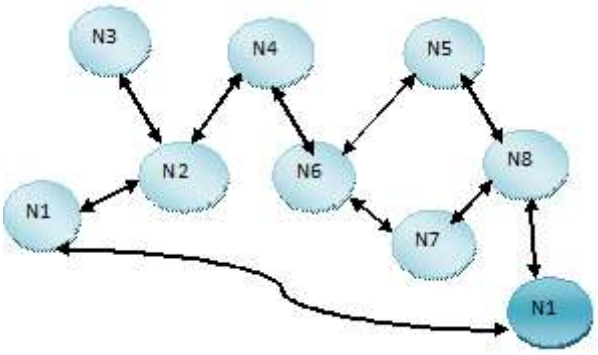

Figure 3: DSDV Protocol

Consider the figure 3 which describes the operation of DSDV protocol.As already mentioned that the routing table contains destination address, sequence number and number of hopes required to reach destination.. Table 1 depicts structure of the forwarding table maintained at node N4. Let us suppose that the address. of each node is represented as Ni and the sequence numbers are denoted by SNNN_Ni, where Ni defines the node that creats the sequence number & SNNN is the value of sequence number.The entries in routing table are before N1 moves away from N2. There is another field in routing table called as install time field which specifies when to delete stale routes. From table it can be concluded that there is no broken link between the nodes as all of the sequence number have even digits in the units plac

Table 2 : Routing Table used in DSDV Protocol

Destination	Next Hop	Sequence Number	Install Time
N1	N2	S406_N1	T001_N4
N2	N2	S128_N2	T001_N4
N3	N2	S564_N3	T001_N4
N4	N4	S710_N4	T001_N4
N5	N6	S392_N5	T002_N4
N6	N6	S176_N6	T001_N4
N7	N6	S028_N7	T002_N4
N8	N6	S050_N8	T002_N4

Now suppose that N1 moves into the neighbor of N5 and N7, and moves away from other nodes mainly N2 as shown with blue nodeThen there will be change in the routing table.

Since in this protocol routes to all the nodes in the network are discovered in advance. This increases the overhead and so decreases the throughput of network. Also all nodes needs to be active all the times as they contains routing tables even if some nodes are not taking part in the process thus a lot of energy is wasted. A large number of control packets are transferred between nodes even if the network is idle. This creates a serious problem[15].This can be overcome by using sleep mode in Ad-hoc networks which consumes less power than idle mode.There are four modes in which network interface hardware at receiver node can be operated.

Transmit mode: When node goes to transmit packet to other neighboring node.
Receive mode: When a node receive a packet from nearby node.

Idle mode: When a node neither transmits nor receives the packet. Idle mode still consumes power as the node has to listen continuously to the network in order to detect the packet.
Sleep mode: It consumes very less power. In this mode , node neither transmits nor receives packet. The node must be changed to idle mode first by explicit information from the node.

Reactive Protocols (Demand-Based Approach)

- Determine route if and when needed
- Source initiates route discovery
- Example: AODV (Ad-Hoc on demand distance vector)

AODV (Ad-Hoc on demand distance vector) is a source initiated routing protocols. It is a reactive protocol as it only requests a route when needed and does not require nodes to maintain routes to the destinations that are not actively used in communication. Routes are maintained only when they are needed by the source. Freshness of routes and loop-free routing is guaranteed with the help of sequence numbers. One of the important aspects of AODV is that at each node time-based states are maintained and a routing-entry not used recently is expired. If a route is broken then neighbors can be notified.Each routing table entry contains destination address , next hop, number of hops, destination sequence number, active neighbors and life time [16].
The main control messages are :

Route request Packet (RREQ): When a node in the network wants to send data to an unknown destination in the network or outside the network, it broadcasts the RREQ packet to all its neighbors. Neighbors will further send to their neighbors till the destination node is not found or lifespan has finished.

Source Address	Request ID	Source sequence number	Destination Address	Destination Sequence number	Hop Count

Figure 4: Route request Packet (RREQ)

Each time the node requests for a new route , request ID is incremented by one thus source address & request ID both uniquely identify new RREQ. On receiving a RREQ message each node checks the source address and the request ID. Now if the receiving node already has RREQ with same values that packet will be discarded else it will be either forwarded replied by destination node with a RREP message. Another case can be that if the source node has no route for destination node, or route is not up-to-date or fresh route, the RREQ will be broadcasted again with incremented hop count and if the node has a route with a sequence number greater than or equal to that of RREQ, a RREP message will be generated and sent back to the source. There is a limitation on the number of RREQ messages send by a node per second.

Route reply packet (RREP): When the destination node receives the RREQ packet ,it reply back using RREP packet by unicast. Life time is the time for which packet remains in the network.The format of RREP packet is shown below

Source Address	Destination Address	Destination Sequence number	Hop Count	Life Time

Figure 5 : Route reply packet (RREP)

Route Error packet (RERR): During communication or path discovery in the network, the nodes monitor their neighboring nodes for any error. When a node is in an active route and lost its link to other nodes, a route error message (RERR) is generated in order to notify the other neighboring nodes on both sides of the link of the loss of this link.
HELLO messages: These messages are generally local broadcasts which are used by all nodes to know about their neighborhood. Nodes neighboring nodes are those with which a node can communicate directly. In AODV these HELLO messages are used to inform the neighbors that the link is still alive. The HELLO messages will never be forwarded

Hybrid Protocols

Hybrid protocols are combination of reactive & proactive protocols. They combines the properties of reactive & proactive protocols.

- Adaptive protocol
- Combination of proactive and reactive
- Example : ZRP (zone routing protocol)

The ZRP hybrid protocol is basically introduced so as to reduce the control overhead used in proactive protocols such as DSDV and to reduce the latency introduced by route discovery in reactive protocols such as AODV. The Zone Routing Protocol (ZRP) as defined in [17] tries to remove these limitations by combining both proactive and reactive protocols.

In a MANET it can be safely assumed that mostly communication takes place, in case of MANETS is between nodes who are close to each other. The new hybrid protocol works in zones i.e. intra zone and inter zone. This new protocol reduces the proactive scope to a zone centered on each node and reactive approach outside the zone. Whenever the source node wants to send packet to destination node, firstly it check the zone of the destination node whether it is within the zone or outside. If destination node is within the zone, the packet has to be routed proactively and Intra-zone Routing Protocol (IARP) is used else Inter-zone Routing Protocol (IERP) is used [18]. In IARP protocol, the route to a destination within the local zone is established with the help of proactively cached routing table and it can be assumed that packet may be delivered immediately. Similarly, outside the local zone, route discovery is done reactively using IERP.

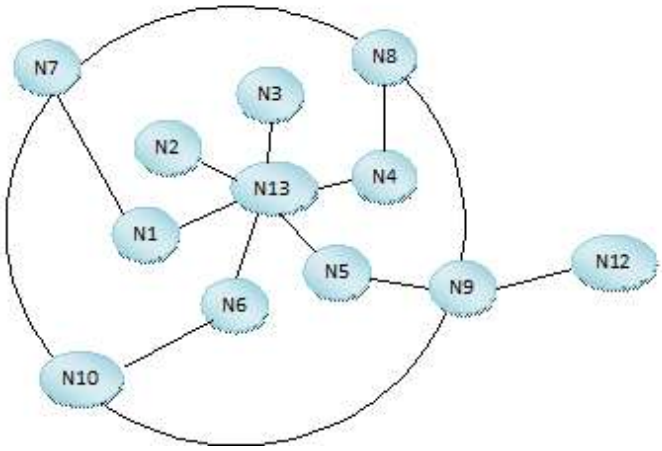

Figure 6 : ZRP Protocol

The source node sends route request to the border nodes of its zone. The request includes its own address, the destination address and a unique sequence number. Now if the destination node is a member of the local zone, it will send route reply packet on the reverse path back to the source else the destination node is not a member of local zone of the source and the border node of the zone will add its own address to the route request packet & forwards the packet to its own border nodes [18]. The source node uses this path saved in the route reply packet to transmit packets to the destination node.

The routing zone of a node is the area of local neighborhood of that node. The "size" of a zone is determined by a radius of length X where, X is the number of nodes lies within the perimeter of the zone. It may be possible that node lies within multiple overlapping zones, and each zone can be of a different size. For example in Figure 1.1, the routing zone of node N13 includes the nodes N1–N9, but not N12.The nodes are divided as peripheral nodes and interior nodes. If the distance of a node to the central node is equal to the zone radius X it is termed as peripheral node else the distance is less than X and called as interior nodes. In Figure 6, the nodes N1–N6 are interior nodes; the nodes N7–N10 are the peripheral nodes and the node N12 is outside the routing zone.

DSR: The Dynamic Source Routing Protocol

The Dynamic Source Routing protocol (DSR) is specially designed for multi-hop wireless ad hoc networks. DSR does not require any existing network infrastructure and is completely self-organizing and self-configuring network. DSR consists of two mechanisms Route Discovery and Route Maintenance. Both mechanisms work together to discover new routes and maintain source routes to destinations in ad hoc network. The source routing allows loop-free routing, avoids any need of up-to-date routing information used by intermediate nodes for forwarding packets. The protocol operates entirely on-demand, and requires the packet overhead of DSR only when there is need to react to changes in the routes currently in use. As already mentioned DSR protocol is composed of two mechanisms Route Discovery and Route Maintenance that work together in the ad hoc network [19].

Route Discovery mechanism is used when the source node S wants to send a data packet to destination node D and S does not know the route to node D. S places a source route in the header of packet which gives the sequence of hops that the packet has to follow to reach D.firstly S will search in its Route Cache i.e. previously learned routes. If no route found, it will initiate route discovery.

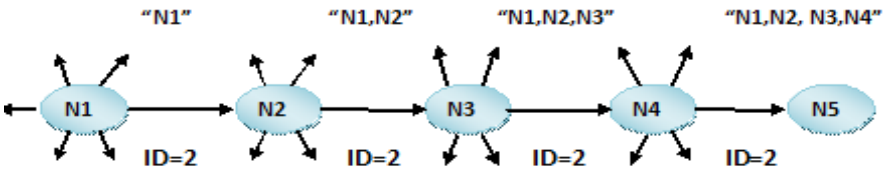

Figure 7: Route Discovery mechanism

Consider an example in fig where node N1 discovers a route to node N5. To initiate, N1 broadcast a ROUTE REQUEST message which is received by all nodes within wireless transmission range of N1. The message contains address of sender, receiver, a unique request id, and a record list containing addresses of each intermediate node to which this message has been forwarded .When another node receives the message, if it is the destination node, it sends a ROUTE REPLY message and a copy of the route record to sender. The sender save this in its Route Cache so that it can be used to send subsequent packets to this destination or else, if the node receiving the ROUTE REQUEST has already another message from same sender with same request id, or it finds its own address in the route record list, it discards the REQUEST. Otherwise, the node adds its own address to the route record in the ROUTE REQUEST message and transmits it as broadcast packet with the same request id as shown in figure. In the ROUTE REPLY node N5 is replying back to N1. Node N5 will analyse its own Route Cache for a back route to N1, and if found, will use it for the source route for delivery of the packet containing the ROUTE REPLY else it will do its own Route Discovery for target node N1, Node N5 could also reverse the sequence of hops as in the route record to send in the ROUTE REPLY message.

Route Maintenance mechanism is used when node S is able to find route to destination node D but it checks weather the link along the route works properly or not. When it indicates that link has been broken, source node S will attempt to use another route to D, or again call up Route Discovery to find a new route. The mechanism is used when S is actually sending packets to D.

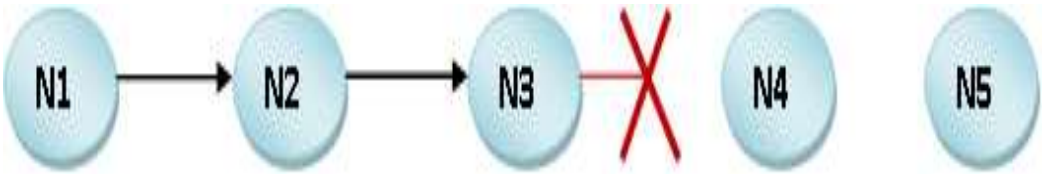

Figure 8: Route Maintenance mechanism

When a packet is forwarded using a source route, each node in the route is responsible for confirming that the packet has been received otherwise packet is retransmitted to confirm the receipt. For example in Figure node N1 has send a packet to node N5 using a source route include N2,N3 and N4 nodes. So node N1 is responsible to get receipt of the packet at N2, N2 is responsible to get receipt at N3 and so on. If these confirmation mechanisms are not available, N1 may set a bit in the packet's header in order to request a DSR-specific software acknowledgement by the next hop in the route. If the packet is retransmitted by some node in the route the maximum number of times as is the case with node N3 and no confirmation is received, N3 will returns a ROUTE ERROR message to N1 which includes the link

that has ben broken and packet could not be forwarded. On receiving ROUTE ERROR message Node N1 removes broken link from its cache. To retransmit the packet or other packets to same node N5, node N1 will find another route in its cache and send the packet using this new route immediately or it may perform a new Route Discovery for the destination node. The main advantages of using DSR are it does not require any periodic packets , periodic routing advertisement, link status packets & neighbor detection packets and due to absence of all these packets the number of overhead packets are reduced to nearly zero.

COMPARISON OF ROUTING PROTOCOL

This section compares the various properties of protocols already discussed in section 3

Table 3 : Comparison of routing protocols

S. No.	Property	DSDV	DSR	AODV	ZRP
1.	**Table driven/ Source Routing**	Table driven	Table driven	Table driven & source routing	Table driven
2.	**Route Mechanism**	Route table with next hop	Complete route cached	Route table with next hop	Route table with next hops
3.	**Network suitability**	For less number of nodes	Up to 200 nodes	Highly dynamic	Up to 1000 nodes
4.	**Route discovery**	Periodic	On demand	On demand	Selective route discovery
5.	**Reactive**	No	Yes	Yes	Partially
6.	**Packet Size**	Uniform	Non-Uniform	Uniform	Non-uniform
7.	**Need of Hello message**	Yes	No	Yes	Yes
8.	**Periodic Broadcast**	Yes	Yes	No	Yes
9.	**Multicast**	No	Yes	No	No
10.	**Power Conservation**	No	No	No	No
11.	**Loop Free**	Yes	Yes	Yes	Yes

CONCLUSION & FUTURE SCOPE

This research is dedicated to the analysis of different types of protocols, used in Wireless Sensor Networks. The main aim of the research is to provide a clear view of the protocols so that by using efficient protocol future researchers can design a much more secure & power efficient network. We have considered some parameters for our analysis; future researcher can be continued by adding some more parameter for analysis. This research would be very helpful for researchers and network designers.

REFERENCES

[1] Asmae BLILAT, Anas BOUAYAD, Nour el houda CHAOUI, Mohammed EL GHAZI (2012) "Wireless Sensor Network: Security Challenges", IEEE, 2012, pp. 68-72.
[2] Daniel E. Burgner, Luay A. Wahsheh (2011) "Security of Wireless Sensor Networks", Eighth International Conference on Information Technology: New Generations, 2011, pp. 315-320.
[3] D.G Anand, Dr. H.G. Chandrakanth, Dr. M.N. Giriprasad (2012) "Security Threats & Issues in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 1, Jan-Feb 2012, pp. 911-916.
[4] Dr. Banta Singh Jangra, Vijeta Kumawat (2012) "A Survey on Security Mechanism and Attacks in Wireless Sensor Networks", International Journal of Engineering and Innovative Technology (IJEIT), Vol. 2, Issue 3, September 2012, pp. 291-296.

[5] Dr. G. Padmavathi, Mrs. D. Shanmugapriya (2009) "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Networks", International Journal of Computer Science and Technology (IJCSIS), 2009, Vol. 4, No. 1 & 2.
[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci (2001), "Wireless sensor networks: a survey" , School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332 USA, 20 December 2001
[7] JA Garcia-Macias and Javier Gomez, "MANET versus WSN", Electrical Engineering Department, National University of Mexico, Ciudad Uni versitaria, Coyoacan, C.P. 04510, D. F. Mexico
[8] Asma Tuteja ,Rajneesh Gujral and Sunl Thalia (2010) , "Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2" ,International Conference on Advances in Computer Engineering, 2010.
[9] Lin, J.; Liu, Y.; Ni, L.M. SIDA: Self-organized ID Assignment in Wireless Sensor Networks (2007). In Proceedings of the 4th IEEE International Conference on Mobile Ad-hoc and Sensor Systems Conference (MASS), Pisa, Italy, October, 2007.
[10] Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas (2009), "Routing Protocols in Wireless Sensor Networks", october 2009.
[11] Zhou H, Mutka M.W. and Ni L.M, "Reactive ID Assignment for Sensor Networks", IEEE International Conference on Mobile Ad-hoc and Sensor Systems.
[12] C.Hedrick,Routing Information Protocol. RFC 1058, June 1988.
[13] Guoyou He , "Destination-Sequenced Distance Vector (DSDV) Protocol" Networking Laboratory, Helsinki University of Technology
[14] Charles.E.Perkins,Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers" University of Maryland, college park, MD20742
[15] Nayan Ranjan Paul, Laxminath Tripathy and Pradipta Kumar Mishra (2011), "Analysis and Improvement of DSDV Protocol" , IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011
[16] Prashant Kumar Maurya, Gaurav Sharma, Vaishali Sahu, Ashish Roberts, Mahendra Srivastava (2012), "An overview of AODV protocol" (IJMER) Vol.2, Issue.3, May-June 2012 pp-728-732
[17] Natasha Dhiman, Jagtar Singh(2013), "Implementation of Zone Routing Protocol using NS2 Simulatot" ,IJARCSSE Vol3, Issue 10,October 2013
[18] Niroj Kumar Pani (May 2009), "A Secure Zone based Routing protocolfor Mobile Ad-hoc Neworks", Department of computer Science & Enggineering,National Institute of Technology, Rourkella, Orrisa,May 2009
[19] David B. Johnson David A. Maltz Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891