ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 2, Issue 8, August 2013

Security Enhancement in AODV Routing Protocol

RaviKumar M Inamathi
Department of computer science
Basaveshwar Engineering College,Bagalkot
University of viveshwaraya technology
Belgaum,Karnataka,India

S. V. Saboji
Department of computer science
Basaveshwar Engineering College,Bagalkot
University of viveshwaraya technology
Belgaum,Karnataka,India

***Abstract*—Adhoc networks are a new wireless networking paradigm for mobile hosts. Mobile Ad-hoc Networks (MANETs) are wireless networks with absence of infrastructure centralized support. Routing in MANETs is challenging task due to mobility of nodes. Several routing protocols have been developed for Mobile Ad-hoc Networks. This paper describes concept of security enhancement in AODV routing protocol by detection and tolerance of attacks using secure message transmission (SMT) protocol. Present AODV routing protocol is not secure by malicious nodes. One main challenge in design of these networks is their vulnerability to security attacks. In this paper we study how to make node malicious and at same we will detect malicious node in AODV protocol using Network Simulator-2(NS-2).**

***Key-words*—AODV, AdHoc, NS-2.**

INTRODUCTION

Mobile ad hoc networks (MANETs) have become a prevalent research area over the last couple of years. Many research teams develop new ideas for protocols, services, and security applicable for these type of networks. This is mainly due to the specific challenges and requirements MANETs pose on the protocols and mechanisms used. They require new concepts and approaches to solve the networking challenges. MANETs consist of mobile nodes which can act as sender, receiver, and forwarder for messages. They communicate using a wireless communication link e.g. a Wireless LAN (WLAN) adapter (IEEE 802.11). These networks are subject to frequent link breaks which also lead to a constantly changing network topology. Due to the specific characteristics of the wireless channel, the network capacity is relatively small. Hence, to be able to use MANETs with many nodes, very effective and resource efficient protocols are needed.

Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks. The structure of the network changes dynamically due to mobility of nodes, interference and path loss. Nodes in these networks utilize the same random access wireless links, cooperating in an intimate manner to engaging themselves in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to and from other nodes in network. Since the nodes are independent to move in any direction, there may be frequent link breakage. In MANET all network activities like discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes. The performance of nodes in ad-hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile nodes can directly communicate to those nodes that are in radio range of each other, whereas others nodes need the help of intermediate nodes to route their packets.

Routing in MANETs is challenging task due to mobility of nodes. Routing is the process of finding desire destination and transferring information to required destination. There may be many attacks like denial of attack, black hole attack etc during transmission of data. so security is main task to detect these attacks. Several routing protocols have been developed for Mobile Ad-hoc Networks. This paper describes concept of enhancement in detection and tolerance of attacks using secure message transmission (SMT) protocol. Here we propose the secure message transmission (SMT) protocol to safeguard the data transmission against arbitrary malicious behavior of network nodes. SMT is a lightweight, yet very effective, protocol that can operate solely in an end-to-end manner. It exploits the redundancy of multi-path routing and adapts its operation to remain efficient and effective even in highly adverse environments. Here we compare and evaluate performance of normal AODV and with SMT protocol AODV.

MANETs dealing with many challenges while designing protocols. There are routing, security and reliability, Quality of service, inter-networking, power consumption.

Routing: Routing is one of the major issue, Since the topology of the network is constantly changing, the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multi cast routing is another challenge because the multi cast tree is no longer static due to the random movement of nodes within the network. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

Security and Reliability: In addition to the common vulnerabilities of wireless connection, an ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets. The feature of distributed operation requires different schemes of authentication and key management. Further, wireless link characteristics introduce also reliability problems, because of the limited wireless transmission range, the broadcast nature of the wireless medium, mobility-induced packet losses, and data transmission errors.

Quality of Service (QoS): Providing different quality of service levels in a constantly changing environment will be a challenge. The inherent stochastic feature of communications quality in a MANET makes it difficult to offer fixed guarantees on the services offered to a device.

Inter-networking: In addition to the communication within an ad hoc network, inter-networking between MANET and fixed networks (mainly IP based) is often expected in many cases. The coexistence of routing protocols in such a mobile device is a challenge for the harmonious mobility management.

Power Consumption: For most of the light-weight mobile terminals, the communication-related functions should be optimized for lean power consumption.

In this paper we study comparison of normal MAODV and SMT protocols in terms of performance metrics such as overhead, Total overhead, packet delivery ratio by varying number of connections. The simulation is carried out using Network Simulator-2.26, awk scripts are used to calculate values of performance metrics.

In order to establish routes between nodes which are farther than a single hop, specially configured routing protocols are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology.

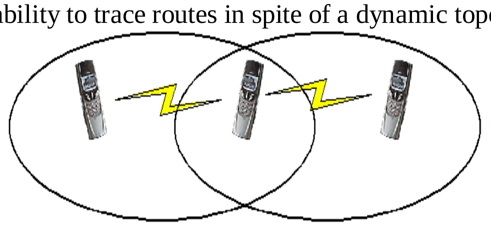

Figure 1 Infrastructure less networks

Figure 1 illustrates a simple 3-node ad-hoc network. In this figure, a source node wants to communicate with a destination node. Source and Destination are not within transmission range of each other. Therefore, they both use the relay node R to forward packets from one to another. So, even though R is primarily a host, R is acting as a *router* at the same time.

LITERATURE SURVEY

The following list of papers discuses routing in ad-hoc network:

The paper [1] explain Secure routing protocols for mobile ad hoc networks which are vital to proper wireless network operation. Unfortunately, ad hoc protocol security properties are often unknown and difficult to analyze. The paper [2] surveys research in service advertising, discovery and selection for mobile ad hoc networks and related issues. It includes a categorization of service discovery architectures for MANETs and their modes of operation, presenting their merits and drawbacks.

The paper [3] gives review of protocols with a particular focus on security aspects. The protocols differ in terms of routing methodologies and the information used to make routing decisions. The paper [4] deals energy conservation and scalability are probably two most critical issues in designing protocols for multi hop wireless networks, because wireless devices are usually powered by batteries only and have limited computing capability while the number of such devices could be large.

The paper [5] explains Mobile Ad-Hoc Networks (MANETs) are particularly useful and well-suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery. The paper [6] deals with for broadcast operation in wireless ad hoc network to prevent collision and achieve low latency at the same time. Here it discuses a greedy broadcast scheduling algorithm based on the graph theory of Maximum Weight Independent Set (MWIS) problem.

The paper [7] it analyzes the robustness of the original AODV and AODV-BR and pointed out their shortcomings. In this paper, we analyze the Ad-hoc On-demand Distance Vector (AODV) routing protocol. Then it explains a Robust AODV protocol, where the route is built on demand and maintained by locally updating route information. The paper [8] deals with two routing protocols named DSDV and AODV are simulated and compared under specific scenarios with WSNs environment.

The paper [9] explains mobile ad hoc networks, there is no centralized infrastructure to monitor or allocate the resources used by the mobile nodes. The absence of any central coordinator makes the routing a complex one compared to cellular networks. The paper [10] presents the modifications of the AODV protocol for dynamic ad-hoc networks. With this modification, they can achieve loner lifetime with stable route without any central information about topologies or traffic demands.

ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 2, Issue 8, August 2013

MOBILE AD-HOC NETWORKS (MANETS)

Mobile Ad-hoc networks are self-organizing and self-configuring multi-hop wireless networks. The structure of the network changes dynamically due to mobility of nodes, interference and path loss. Nodes in these networks utilize the same random access wireless links, cooperating in an intimate manner to engaging themselves in multi-hop forwarding. The node in the network not only acts as hosts but also as routers that route data to and from other nodes in network. Since the nodes are independent to move in any direction, there may be frequent link breakage. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multihop forwarding. The node in the network not only acts as hosts but also as routers that route data to from other nodes in network.

In MANET all network activities like discovering the topology and delivering messages must be executed by the nodes themselves. Hence routing functionality will have to be incorporated into the mobile nodes . The performance of nodes in ad-hoc networks is critical, since the amount of available power for excessive calculation and radio transmission are constrained. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile nodes can directly communicate to those nodes that are in radio range of each other, whereas others nodes need the help of intermediate nodes to route their packets. Nodes A and C must discover the route through B in order to communicate.

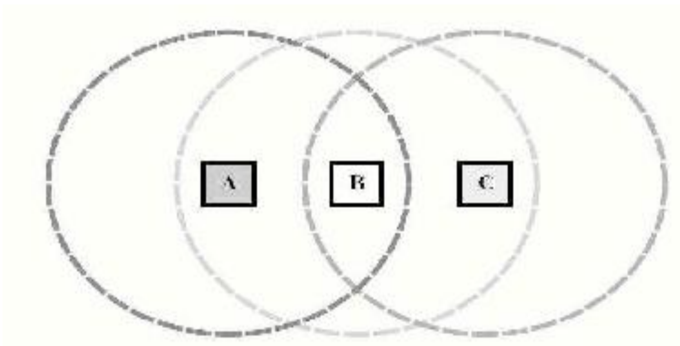

Figure 2: Simple ad-hoc network with three participating nodes

Nodes are furnished with wireless transmitters and receivers using antennas, which may be highly directional, Omni-directional. At a given point in time, depending on positions of nodes, their transmitter and receiver coverage patterns, communication power levels, "ad-hoc" network exists among the nodes. This ad-hoc topology may modify with time as the nodes move or adjust their transmission and reception parameters.

ROUTING IN MANETS

A wireless *mobile ad-hoc network (MANET)* is a network consisting of two or more mobile nodes equipped with wireless communication and networking capabilities, but lacking any pre-existing network infrastructure. Each node in the network acts both as a mobile host and a router, offering to forward traffic on behalf of other nodes within the network. For this traffic forwarding functionality, a routing protocol is needed.

Routing is the process of selecting paths in a network along which to send network traffic. In packet switching networks, routing directs packet forwarding, the transit of logically addressed packets from their source toward their ultimate destination through intermediate nodes. An ad hoc routing protocol is a convention, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad-hoc network.

As shown in figure 3 the process of finding shortest path in which minimum path is taken to reach the destination. It makes clear idea about how MANETs work and routing will take place for finding minimum shortest path.

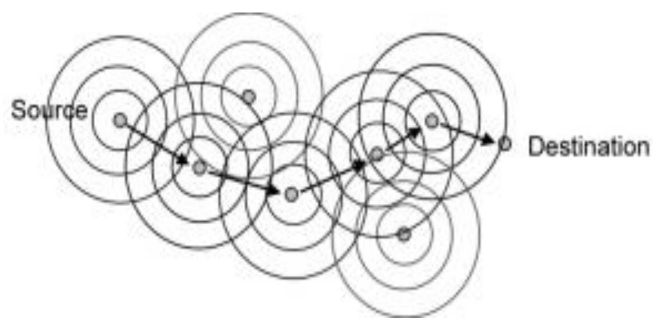

Figure 3 shortest path

PROPOSED ALGORITHM

In our proposed algorithm enhancement of AODV made with secure message transmission using SMT Agent by enabling multicast operation (MAODV).

Algorithm MAODV with SMT protocol

1. Start at source, Multicast RREQ to nodes, to pass message through their neighbors to nodes with which they cannot directly communicate.
2. MAODV does this by discovering the routes along which messages can be passed by Multicast operation.
3. Initialize Active Path Set →(APS) operation, the two communicating end nodes make use of a set of diverse, preferably node disjoint paths that are deemed valid at that time.
4. **S**ource start updating APS Rating.
5. At intermediate nodes, verify destination sequence no.

   If dest. Seq. No. (Node) < dest. Seq. No. (packet):

Update routing table entry with this path and broadcast this packet
Else send RREP to source.

6. SMT protocol gets operated if any unknown behavior.
7. Any attacks detected, SMT agent sends ACK to tolerate from attacks.
8. Successful messages are received from destination; If not then route is broken or compromised.
9. If node gets more than one RREQ from same source then:
   If node! = destination
   Discard RREQ
   If node=destination
   Process RREQ
10. Stop APS Operation.
11. Reconstruct Message as Original using Security Association (SA) by MAC.
12. Compare all RREQ at destination on some attribute value like latency or number of hops and selects RREQs to process and discard rest.
13. Create RREP for all collected RREQ and process them towards source.
14. At intermediate nodes, for multiple entries by RREP from same destination, preserve the entries coming from different nodes, delete rest duplicate entries.
15. At source node after getting multiple RREP
    Forward data using single path.
    Forward data using multiple paths.
16. If RERR is received by source for some path, Delete the entry of concerned path from routing table. Consider the other path as primary or as needed.
17. Stop SMT Protocol.
18. Step 1 continues for next Communication.

Above algorithm explains working of MAODV with SMT protocol for secure data transmission over the network. It consists of step by step procedure from starting route discovery to end of transmission of data to desire destination.

In multicast environment there are many groups. Each group contains nodes, nodes called member of that group. Among which contain group leader for each group and group leader maintain members within that group. So RREQ is sent to all group leaders, leader will find destination within that group.

Initially whenever request is given to source to find destination it will initiate the RREQ, which contains destination address, source address and destination sequence number of packet to be sent to find destination. This process is called route discovery. In multicast RREQ sent to all group within that network, such that it will sent to all other members within that group.

With SMT, at any particular time, the two communicating end nodes make use of a set of diverse, preferably node disjoint paths that are deemed valid at that time. We refer to such a set of paths as the active path set (APS). The source first invokes the underlying route discovery protocol, updates its network topology view, and then determines the initial APS for communication with the specific destination. Sequence number of each packet is compare with sequence number present in routing table to avoid loops within network.

Simulation Results:

The algorithm MAODV evaluated with NoAttack, Attack and Detect with SMT Protocol. In this analysis network simulator version 2.26 used. Following are the Performance Metrics used to measure using NS-2:

Delivery ratio: The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination. The greater value of packet delivery ratio means the better performance of the protocol.

Overhead: Refers to the time it takes to transmit data of packets in network. Each packet requires extra bytes of format information that is stored in the packet header, which, combined with the assembly and disassembly of packets, reduces the overall transmission speed of the raw data.

Total Overhead: Refers to the total time it takes to transmit data of packets in network. It includes transmission overhead, network overhead, packet overhead, delay overhead etc. These factors make effects to decrease the performance of network while transmitting packets.

Simulation Results of MAODV with NoAttack

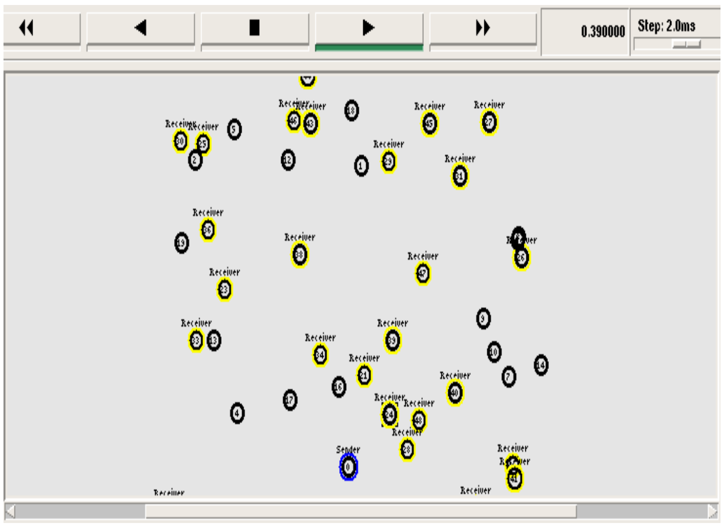

Figure 4:*Initial network scenario with NoAttack*

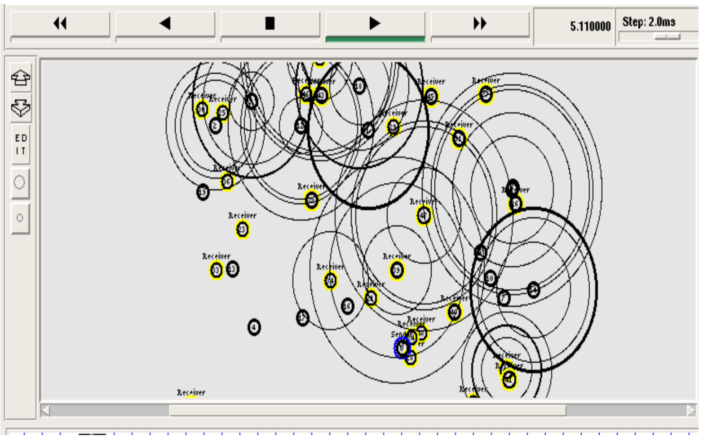

Figure5:Simulation scenario

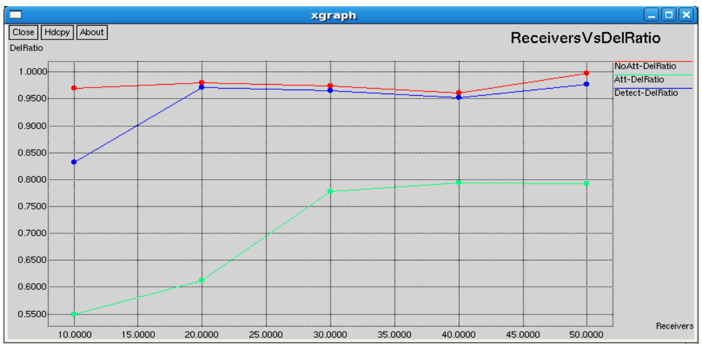

Figure 6:Average Delivery vs Receivers of MAODV and SMT

As shown in above figure 6 results are taken with respective without any Attack of malicious behavior with varying number of connections(10,20,30,40,50). Results outcome with performance of MAODV with respective to the Delivery Ratio, Overhead, and Totaloverhead.In which above graph is plotted with Delivery ratio performance metric. As above graph is plotted with Receiver vs Delivery Ratio of NoAttack, Attack and Detect. In which delivery ratio of NoAttack and Detect gives near same view. In detect it gradually increase because it take time initially to detect unbehavior, node. But in Attack status between 10 and 20 node mobility is very low due to the dropping of packets. So after 20th node delivery ratio again improved.

Simulation Results of MAODV with Attack

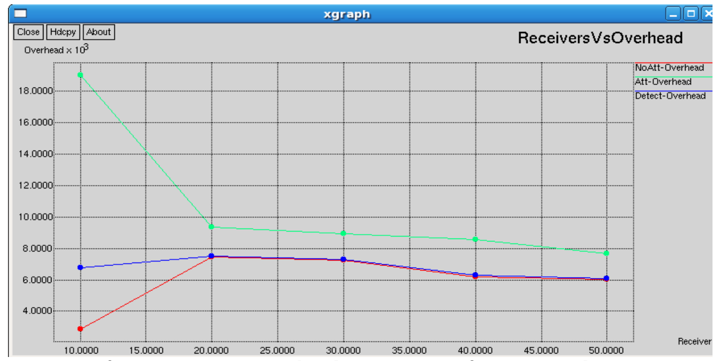

figure 7:*Average Overhead vs Receivers of MAODV and SM*

As shown in above figure 7, results are taken with respective with Attack of malicious behavior with varying number of connections(10,20,30,40,50).Results outcome of performance of normal AODV with respect to the Delivery Ratio, Overhead, and Total overhead. In which above graph is plotted with Overhead performance metric. According to above results graph is plotted with Receiver vs Delivery Ratio of No Attack, Attack and Detect. In which over congestion of packets Overhead is high with Attack.

Simulation Results for MAODV with SMT Detect

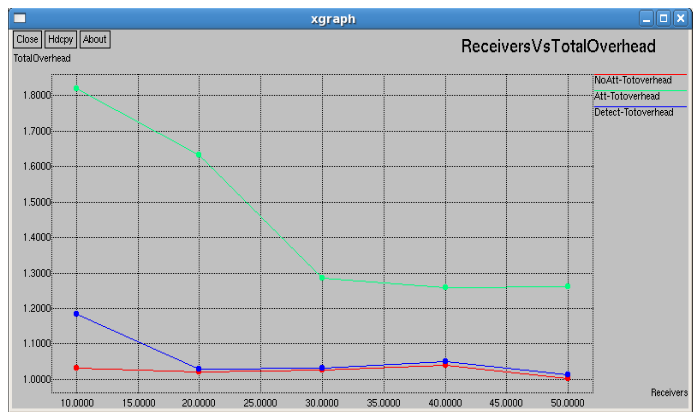

Figure8:Average Totaloverhead vs Receivers of MAODV and SMT

As shown in above figure 8, results are taken with respective with Detection of malicious behavior with varying number of connections(10,20,30,40,50).Results outcome of performance of SMT with respective to the Delivery Ratio, Overhead, and Total overhead. In which above graph is plotted with respective Total overhead performance metric. According to above results graph is plotted with Receiver vs Total overhead of NoAttack, Attack and Detect. In which over congestion of packets Total overhead is after detection of malicious nodes with Attack. But as compare to MAODV the ourcome of SMT after detection of attacks is same. Because initially nodes to be detected due to this some congestion initial it will take time with low total overhead.

CONCLUSION

In this work we have made normal unicast AODV to Multicast AODV operation in which SMT Agent is implemented to detect attacks and results can be extracted in terms of Delivery Ratio, Overhead and Total overhead. Simulation results are taken using Network Simulator 2.26 Under scenario varying number of connections. Due to presence of multicast and queues, MAODV show better performance over detecting attackers using SMTAgent. Since routing information is updated and multicast frequently, MAODV with attacks performance degrades as number of connections increases, compared to as that of MAODV without attacks and after detection using SMTAgent. MAODV performs better as high mobility scenarios, low overhead and total overhead from our simulation. So from all analysis we finally conclude that MAODV with SMT protocol implementation is a ideal choice for communication.

The work that has been accomplished in this project is quite flexible, as multiple nodes can be accessed data from Tcl script and bringing the possibility to modify the existing protocols to adapt to multicast support mobile node architecture. One additional aspect would be the extension of whole model so as to really include multicast technologies, and not only multicast belonging to same technology. Another topic would be to address is in our project results are carried out varying only number of connections with random connection, in future we can consider results by varying speed with fixed position so that performance may vary this could also benefit for the new feature. Also multicast operation can be extended for other routing protocol like DSDV, TORA etc.

REFERENCES

[1] Todd R Andel "Surveying security analysis techniques in MANET" IEEE Communication surveys, The Electronic Magazine of Original Peer-Reviewed Survey Articles, vol 9, No4, 2007.

[2] Christopher N. Ververidis and George C. Polyzos, "Service Discovery for Mobile AdHoc Networks", IEEE Communications Surveys & Tutorials, vol 10, No 3, 2008.

[3] Loay Abusalah, Ashfaq Khokhar and Mohsen Guizani "A Survey of Secure Mobile AdHoc Routing Protocols", IEEE Communications Surveys & Tutorials, vol 10, No 4, 2008.

[4] Yu wang, xiang-yang Li, wen-zhan, "Energy Efficient Localized Routing in Random Multihop Wireless Network", IEEE Transactions on Parallel and Distributed Systems, vol 22, No 8, 2011.

[5] Karim ElDefrawy, Gene Tsudik "Privacy-preserving Location based on demand routing in MANETs", IEEE Journal on selected area in communications, vol 29, No 10, Dec 2011.

[6] Wei wang, Boon-Hee Soong, "Collision-free and Low latency scheduling algorithm for Broadcast operation in wireless AdHoc networks", IEEE Communication Letters, vol 11, No 10, Oct 2007.

[7] Suhua Tang and Bing Zhang, "A Robust AODV protocol with local update", ATR Adaptive communications research lab, Japan.

[8] Adel S El asheb, "Performance evaluation of AODV and DSDV routing protocol in wireless sensor network environment", International conference on Computer Networks and Communication Systems, vol 35, 2012.

[9] Humaira Nishat, Vamsi Krishna, "Performance evaluation of AODV and Modified AODV (R-AODV) in MANETs", International journal of Distributed and Parallel Systems, vol 2, No1, Jan 2011.

[10] M.Devi and Dr. V. Rhymend Uthariaraj, "Routing with AODV protocol for Mobile AdHoc network" International Journal of Technology And Engineering System, vol 2, No 1, March 2011.