Computing, Information Systems & Development Informatics Journal
Vol. 10 No. 3, September, 2019 - www.cisdijournal.org

Reduction in High Rate of Packet Drop in Reverse Adhoc On-Demand Distance Vector Routing Protocol Under Wormhole Attack in Mobile Adhoc Networks

[1]Ojo, Adebola K. and [2]Akinnifesi, Akintunde S.
[1,2]Department of Computer Science
University of Ibadan
Ibadan, Nigeria
E-mails: [1]adebola_ojo@yahoo.co.uk, [2]akinnifesiakintunde@yahoo.com
Phones: [1] +2347032736013, [2]+2348065541696

ABSTRACT

Over the years the advent of wireless communication has made Mobile Ad-hoc Networks (MANETs) become more accessible platforms for easier exchange of data especially where it is expensive or impossible to establish fixed network infrastructure. These networks can offer a life-saving communication in a disaster or an emergency situation under well-equipped routing protocol as the quality of service provided by MANETs is dependent on its routing protocol. This dependency has led to the development of several Multi-path routing protocol which guard against drop of unicast Route Reply packet associated with Ad-hoc On-Demand Distance Vector (AODV) - a single-path routing protocol. However, the performance of Reverse-AODV (a Multi-path routing protocol) can be vulnerable to high rate of packet drop under the influence of wormhole attack as the shortest path is selected and maintained for a given expiration time or until path fails. In this paper, we proposed an improved Reverse-AODV routing protocol (iR-AODV) which adopts different path routing; as a way of reducing the impact of wormhole attack on packets during transmission. The study simulated Reverse-AODV routing protocol and the improved version (iR-AODV) under wormhole attack. Both protocols were evaluated by considering different performance metrics under the same parameters such as number of nodes and simulation time. The results showed that the proposed iR-AODV recorded a smaller number of packet drop and higher Packet Delivery Ratio under wormhole attack when compared with R-AODV routing protocol.

Keywords: MANETs, AODV, Reverse-AODV, iR-AODV, performance metrics.

CISDI Journal Reference Format
Ojo, A.K. & Akinnifesi, A.S. (2019): Reduction in High Rate of Packet Drop in Reverse Adhoc On-Demand Distance Vector Routing Protocol Under Wormhole Attack in Mobile Adhoc Networks. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 10 No 3, Pp 1-8. Available online at www.cisdijournal.org. DOI Affix - https://doi.org/ 10.22624/AIMS/CISDI/V10N3P1

INTRODUCTION

The advent of wireless communication has made Mobile Ad hoc Networks (MANETs) (Figure 1) become more accessible platforms for easier exchange of data particularly where it is costly or impossible to establish fixed network infrastructure. These networks offer numerous advantages over traditional (fixed) networks including but not limited to reduced infrastructure costs, ease of deployment and fault tolerance. They are formed by a collection of mobile wireless devices, such as laptop computers, Personal Digital Assistants (PDAs) and wireless phones that communicate with each other without a fixed network infrastructure. Each mobile device in a network serves as a node in MANET and dynamically behaves as router and host. They can be used for a variety of applications. Examples of such applications are military communications, rescue operations as well as an alternative to Internet connectivity; for devices in both rural and urban areas which are temporarily located out of range of an Internet access point (Ding, 2008).

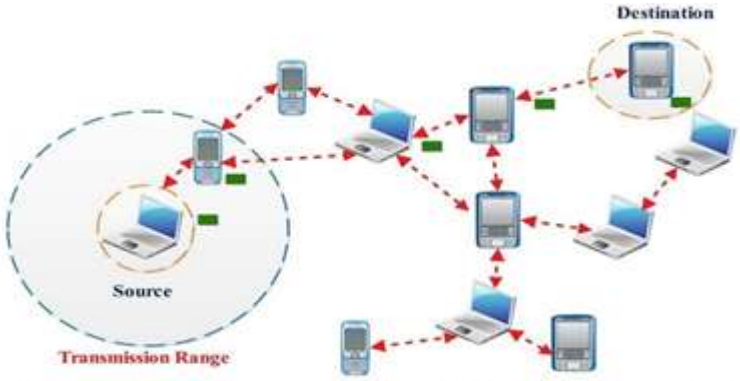

Figure 1: Simple Structure of Mobile Ad Hoc Network (MANET)
(Source: https://www.researchgate.net/publication/286762843)

The transmission of packets from source node to destination node in MANETs is being handled by routing protocol (Chetana *et al*., 2013). Routing protocols can be classified into Proactive, Reactive and Hybrid depending on their functionality. In Proactive protocols, routing information tables are maintained on each node which are updated whenever there is a change in the network topology. Examples are Destination Sequence Distance Vector (DSDV), Open Link Source Routing (OLSR). Reactive Protocols also known as On Demand protocols do not update periodically. The update is done when there is need to send packet through a requested route. This protocol does not consume much resources as in the case of proactive protocol. Examples are Ad hoc On Demand Distance Vector (AODV), Reverse Ad hoc On-Demand Distance Vector and Dynamic Source Routing (DSR). Hybrid protocols on the other hand combine the strength of reactive and proactive routing protocol. In this protocol, nodes are clustered into sections based on their various physical locations or distances from each other. Example is Zone Routing Protocol (ZRP) (Parvathavarthini *et al*., 2013).

The area of discussion in this paper is based on Reverse AODV (R-AODV), a multipath reactive routing protocol that guards against unicast RREP packet loss associated with AODV. The Reverse-AODV broadcasts the route reply packet throughout the network instead of unicasting it. This procedure generates multiple partial or full disjoint paths at the source node for data transmission. (Chonggun *et al.*, 2006). However, the performance of Reverse-AODV (an example of Multi-path routing protocol) can be vulnerable to high rate of packet drop under the influence of wormhole attack as the shortest path is selected and maintained for a given expiration time before another path can be selected. (Sanabani *et al,* 2014)

2. WORKING OF R-AODV ROUTING PROTOCOL

The working methodology of R-AODV routing protocol can be classified into two phases:

1. Route Discovery and;
2. Route Update and Maintenance

2.1 Route Discovery Phase

During the route discovery phase, the source node broadcasts Route Request (RREQ) packet which contains the following information: packet type, source address, destination address, broadcast ID, hop count, source sequence number, destination sequence number and request time (timestamp) to all nodes within its transmission range. These neighbouring nodes then rebroadcast the RREQ to other nodes in the same manner until it gets to the destination node.

As the RREQ is broadcast in the whole network, some nodes may receive several copies of the same RREQ. When an intermediate node receives a RREQ, it checks for redundancy of packets and drops redundant RREQ packets. When the destination node receives the first RREQ packet, it generates and broadcasts the Reverse-Route Request (R-RREQ) packets in order to find multiple reverse paths back to the source node. When an intermediate node receives R-RREQ packet, it creates forward route entry and broadcast R-RREQ packet to its neighbour node within its transmission range. When the source node receives the first R-RREQ packet then it starts packet transmission immediately and stores the other late R-RREQ packet for future use. (Sanabani *et al,* 2014).

2.2 Route Update and Maintenance Phase

According to Saida *et al.*, (2012), the source node upon reception of control packets updates route by comparing the sequence numbers of all received control packets and selects the path with higher sequence number (that is, recent route) as best route but if the sequence numbers are the same, the source node compares the hop count (that is, the number of intermediate nodes between the source and destination node) and selects a path with a smaller hop count. The quality of wireless channel varies over time and as such the best path keeps changing as transmission continues.

The feedback from the MAC layer can be used to detect the connectivity of the link. When a node notifies that its downstream node is out of its transmission range, the node generates a Route Error (RERR) message and sends to its upstream node. If failure occurs closer to the destination node, the node which receives RERR message can attempt local repair; otherwise the nodes forward RERR packet until it reaches the source node. The source node can select an alternative route or initiate a new route discovery procedure.

3. OVERVIEW OF WORMHOLE ATTACK ON ROUTING PROTOCOL

R-AODV routing protocol is not exempted from malicious attack owing to the fact that nodes arbitrarily join and leave the network. Also, the lack of assigned routers allow each node in the network to participate in the routing process. Thus, routing can easily be interrupted by nodes with malicious intentions. Among all possible range of attacks launched in Mobile Ad hoc Networks (MANETs), wormhole attack is one of the most threatening and severe attacks (Wang *et al*., 2006). According to Hu *et al*., (2006), a malicious node captures packets from one location in the network and "tunnels" them to another malicious node at a distant point, which replays them locally. This makes the tunneled packet arrive either sooner or with a lesser number of hops compared to the packets transmitted over normal multihop routes. Hence, it creates a false impression that the two end points of the tunnel are very close to each other. The two malicious end points of the tunnel may use the wormhole (tunnel) to pass routing traffic to attract routes through them. They can then launch variety of attacks against data traffic flowing on the wormhole path such as selective or entire dropping of data packets.

3.1 Wormhole Implementation Method

Wormhole attack can be implemented in two ways:

1. In-band channel: In this approach malicious node consider some other neighbours for packet transmission along them. This is shown is Figure 2 on page 3
2. Out-band channel: This approach does not involve any other neighbor node except wormhole node and transfer packets through themselves only. Hence not letting hop count value to increase by more than one. This is shown in Figure 3.

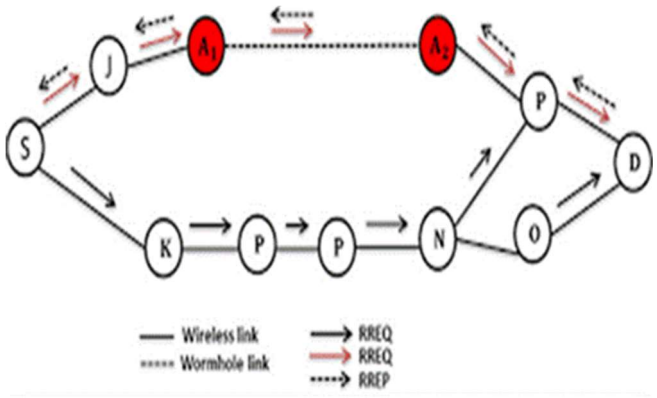

Figure 2: An In-bound Wormhole Attack launched through packet encapsulation in MANETs

Figure 3: An out of bound (Hidden) Wormhole Attack launched through high powered transmission in MANETs

3.2 Various Proposed Related Works on Wormhole Attack

[a] Mary *et al,* (2010), analyzed the performance of reactive multicast routing protocol On- Demand Multicast Routing Protocol (ODMRP) under the influence of wormhole nodes under different scenarios and designed a Worm Hole Secure ODMRP (WHS-ODMRP) by applying certificate-based authentication mechanism in the route discovery process. The proposed protocol reduced the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance.

[b] Gupta *et al,* (2011), proposed an approach, called WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol and considered to detect wormhole attack with the help of hound packets.

[c] Nail-Abdesselam *et al,* (2008) used four message exchanges to defend against wormhole attack in OLSR. This method used Hello and ACK message to confirm the delay

4. PROPOSED WORK

In R-AODV routing protocol, source node selects the shortest path (path with minimum hop count and highest sequence number) for data transmission under the disguise of wormhole nodes with malicious intention for a given expiration time or until path fails (Figure 4). Thus, such routing protocol can be highly vulnerable to wormhole attack. Therefore,

the study proposed a better R-AODV routing protocol, namely Improved Reverse-AODV (iR-AODV) routing protocol which adopts different path routing; as a way of reducing the impact of wormhole attack on packets during transmission. This is shown in Figure 5.

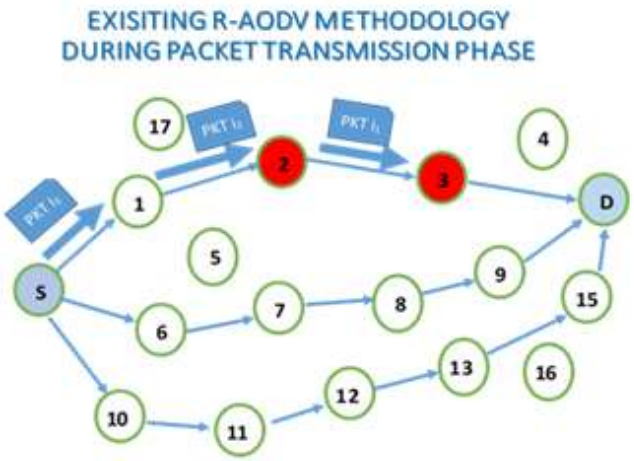

Figure 4: Packet routing via a single path until TTL (Time to Live) elapsed or path fails (Sabani *et al*, 2014)

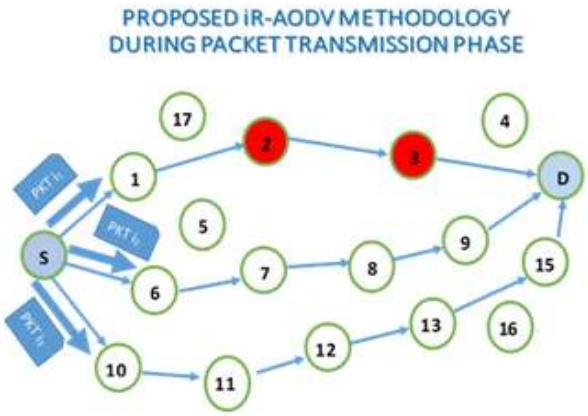

Figure 5: Packet routing via all available paths

The modification of R-AODV routing protocol to iR-AODV (Improved R-AODV) routing protocol was done by extracting R-AODV protocol file into ns-2.35 directory and modification was carried out on the extracted R-AODV.cc, R-AODV.tcl, R-AODV_rqueue.h, R-AODV_rqueue.cc files to allow packet routing via all available routes. Also, the \tcl\lib\ns-lib.tcl library where protocol agents are configured as a procedure was adjusted as well as the \makefile in the root directory of the ns-2.35. After all modifications were done, NS-2.35 was recompiled to create object files. This was done using the following commands:

$] make clean
$] make
$] make install

Subsequently, the study simulated wormhole attack on R-AODV routing protocol (Figure 6) and the improved version (iR-AODV) routing protocol (Figure 7) using NS-2.35 simulator and evaluate the performance of both protocols by considering different performance metrics under the same parameters such as number of nodes and simulation time.

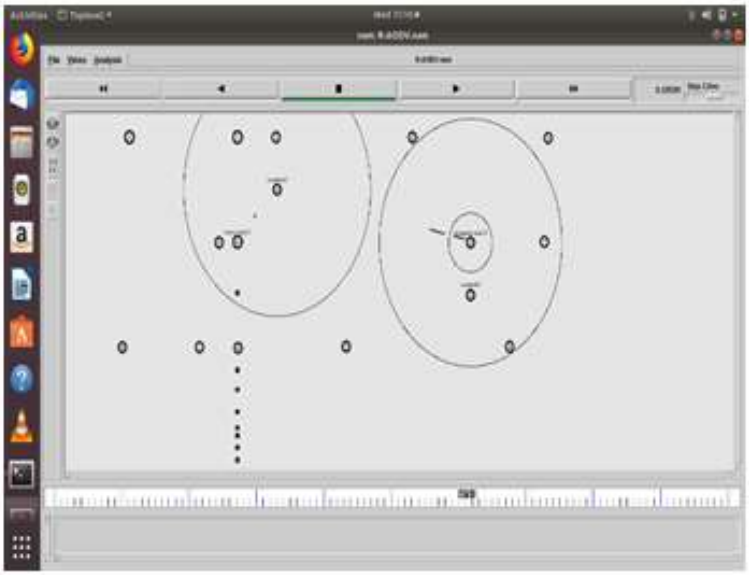

Figure 6: Network Animator (NAM) showing data transmission and packet drop in R-AODV protocol

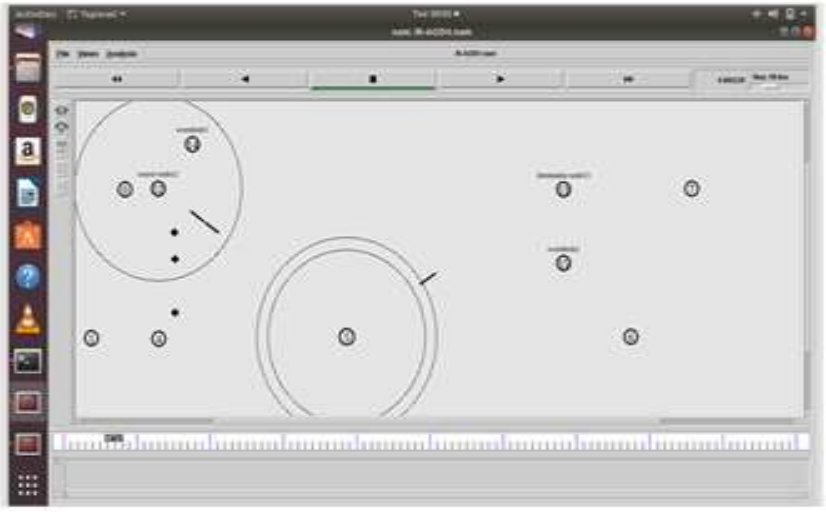

Figure 7: Network Animator (NAM) showing data transmission and packet drop in iR-AODV protocol

Finally, the post simulation process was carried out using awk script to generate result of simulations from trace files (R-AODV.tr and iR-AODV.tr) using the following commands:

~/ex-wormhole-1$ ns awk -f PDR.awk R-AODV.tr → for R-AODV protocol

~/ex-wormhole-1$ ns awk -f PDR.awk iR-AODV.tr → for iR-AODV protocol.

The generated results were produced in form of charts for clear analysis and interpretation of results.

Simulation Parameters
The parameters that were used to carry out the research are presented in Table 1.

Table 1: The Table Showing Mobility Parameters Used for Simulation

Parameters	Value
Simulator	NS-2.35
Data packet size	512bytes
Simulation time	10secs
Number of nodes	16
Data Rate	1MB
Pause Time	5secs
Observation Parameters	Packet drop, Packet delivery ratio and % Packet delivery ratio
No of malicious node	2
Routing Protocols	R-AODV and iR-AODV
Simulation size	500m x 500m

5. RESULTS AND DISCUSSIONS

The results of R-AODV and iR-AODV routing protocol under wormhole attack were compared using the three observation parameters mentioned in Table 1. Figures 8, 9 and 10 respectively show packet loss, packet delivery ratio and percentage packet delivery ratio for R-AODV and iR-AODV routing protocol under wormhole attack.

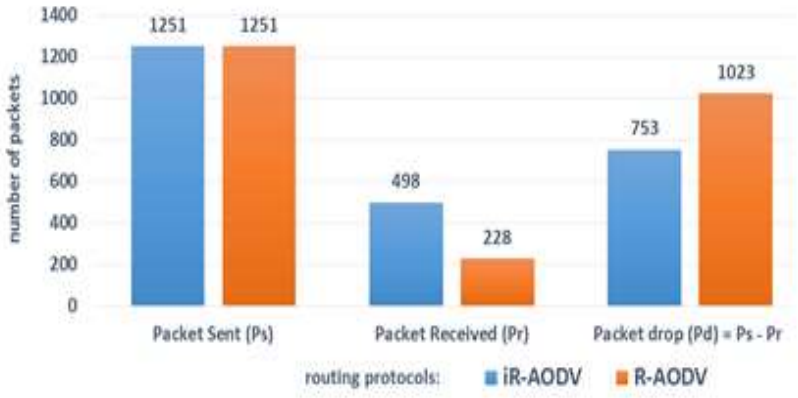

Figure 8: Comparison of Packet Drop in R-AODV protocol under wormhole attack with respect to Packet Sent and Packet Received

Figure 8 shows that the improved R-AODV (iR-AODV) routing protocol recorded lesser packet drop (with 753 packets dropped out of 1251 total packets sent) when compared with R-AODV routing protocol (with 1023 packets dropped out of 1251 total packets sent) under wormhole attack. Figures 9 and 10 show that the improved R-AODV (iR-AODV) routing protocol has better Packet Delivery Ratio of (0.3981) and Percentage Packet Delivery Ratio of (39.8081%) when compared with R-AODV routing protocol with Packet Delivery Ratio of (0.1823) and Percentage Packet Delivery Ratio of (18.2254%). The result is due to the fact that improved R-AODV (iR-AODV) used different paths for data transmission instead of maintaining the same shortest path with wormhole node for data transmission as in the case of R-AODV routing protocol.

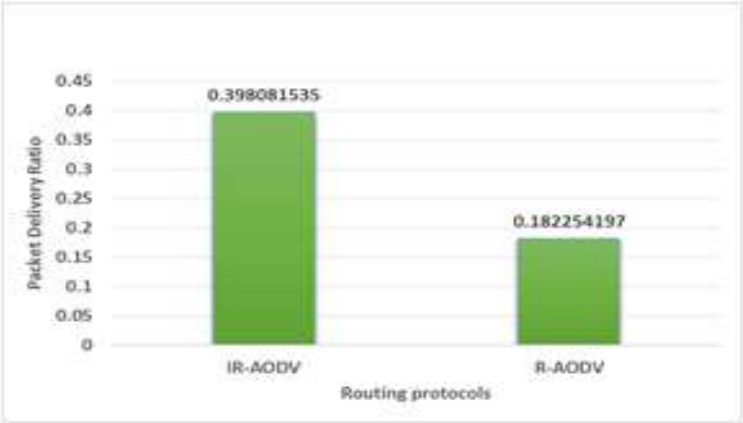

Figure 9: Comparison of Packet Delivery Ratio in R-AODV and iR-AODV protocol under wormhole attack

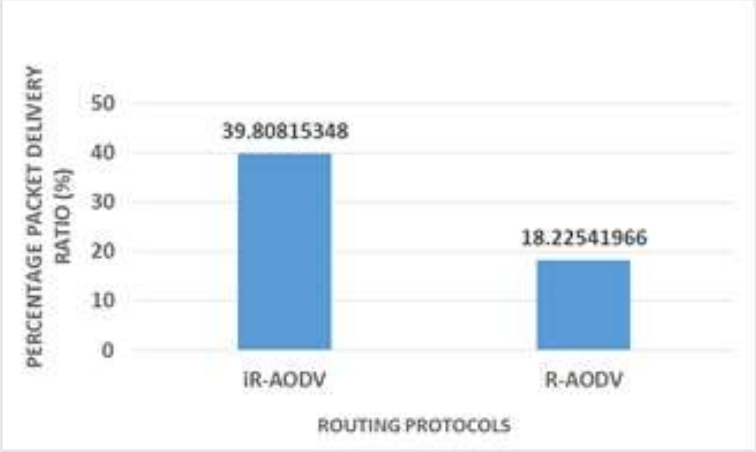

Figure 10: Comparison of Percentage Packet Delivery Ratio in R-AODV and iR-AODV protocol under wormhole attack

6. CONCLUSION AND FUTURE WORK

The study simulated R-AODV routing protocol and the improved version (iR-AODV) under wormhole attack using NS-2.35 simulator and evaluated the performance of both protocols by considering different performance metrics under the same parameters such as number of nodes and simulation time. The simulation results showed that the proposed iR-AODV records lesser number of packet drop and higher Packet Delivery Ratio under wormhole attack when compared with R-AODV routing protocol. In future, similar study can be conducted using different performance metrics such as throughput and end-to-end delay.

REFERENCES

1. Chonggun Kim, Elmurod Talipov and Byoungchul Ahn (2006). A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks," LNCS 4097, pp. 522-531.
2. **Ding, S. (2008). A Survey on Integrating MANETs with the Internet: Challenges and Designs, Computer Communications, Vol. 31, no. 14, pp. 3537-3551.**
3. Farid Naït-Abdesselam, Brahim Bensaou, and Tarik Taleb, (2008). Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks. *IEEE Communications Magazine*. Vol. 46, pp. 127-133.
4. Gupta, S., K. Subrat, and S. Dharmaraja, (2011). WHOP: Wormhole Attack Detection Protocol using Hound Packet. *International Conference on Innovations in Information Technology*, pp. 226-231.
5. Hu Y.C., Perrig, .A. and Johnson, D.B., (2006). Wormhole Attacks in Wireless Networks. IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, pp. 370-380.
6. Mary, A., V. Vasudevan, and A. Ashwini, (2010). A Certificate Based Scheme to Defend Against Wormhole Attacks in Multicast Routing Protocols in MANETs. *IEEE International Conference on Communication Control and Computing Technologies (ICCCCT)*, pp. 407-412.
7. Parvathavarthini and Dr S.S. Dhenakaran (2013). An Overview of Routing Protocols in Mobile Ad-Hoc Network, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, pp. 251-259.
8. Pravanjan Das and Upena D Dalal, "A Comparative Analysis of AODV and R- AODV Routing Protocols in MANETS", International Journal of Computer Applications 72(21):1-5, June 2013.
9. Pravanjan Das, Sumant Kumar Mohapatra and Biswa Ranjan Swain, (2014). A Simulation based Performance Evaluation of AODV, R-AODV and PHR-AODV Routing Protocols for Mobile Ad hoc Networks, *International Journal of Wireless & Mobile Networks (IJWMN)* Vol. 6, No. 5, pp. 165-174.
10. Saida, .M., Maher, .A., A. Tariq, A. Raed, A. Maha and A. Ola, (2012). Comparison Study of Routing Protocols in MANET, *Archives Des Sciences Journal*, Vol. 65, pp. 615-629.
11. Sanabani, M., R. Alsaqour and S. Kurkushi, (2014). A Reverse and Enhanced AODV Routing Protocol for MANETS. *ARPN Journal of Engineering and Applied Sciences*, Vol. 9, No. 2, pp. 153-159.
12. Wang, W., Bhargava, B., Y. Lu, and X. Wu. (2006), Defending against Wormhole Attacks in Mobile Ad hoc Networks. Wireless Communications and Mobile Computing, Vol. 6, No 4, pp. 483–503.