Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

(Special Issue for ITECE 2016)

An Enhanced AODV Routing Protocol W.R.T Security

[1]Shewaramani Jitendrakumar G., [2] Swadas Prashant B., [3]Prajapati Nilesh B.

[1]ME Student, Computer Engineering Department, BVM, V.V Nagar, Gujarat, India
[2]Associate Professor, Computer Engineering Department, BVM, V.V Nagar, Gujarat, India
[3]Associate Professor, Information Technology Department, BVM, V.V Nagar, Gujarat, India

Abstract — MANET has gained immense popularity in recent times because of its self-configuration and self-maintenance capabilities. AODV (Ad-hoc On-demand Distance Vector) is commonly used reactive routing protocol in MANETs for route establishment between communicating nodes. Due to lack of centralized monitoring and dynamically changing topology of MANET, they are highly vulnerable security attacks. Black hole attack is a type of denial-of-service attack in which malicious nodes falsely advertise shortest path to the destination node. AODV protocol directs packets towards those malicious nodes and such nodes drop packets. In this paper, an efficient technique to detect and prevent black hole attack is proposed. Calculated results of various network metrics like PDR, NRL and Avg. End to End Delay are for single black hole attack show up to 80% improvement in PDR.

Keywords- mobile ad hoc network, security, routing, AODV, black hole

I. INTRODUCTION

A mobile ad hoc network (MANETs) is a dynamic, self-organized, self-configuring and infrastructure-less network which consists of several movable nodes who communicate with each other without any centralized authority. Mobile nodes in the network acts as host when requesting or providing information from or to other nodes and acts as router when discovering and maintaining routes for other nodes.

Due to the nature of MANET, they have ability of creating a network in such situations where infrastructure network would be either impossible or very expensive. Applications of MANETs range from military battlefield, disaster relief, medical services, personal area networks, commercial sector and many more [1].

Following are few characteristics of MANET [2, 6]:

- Dynamic Topology: Nodes are free to move arbitrarily and have no restriction on their distance from other nodes. As a result of this random movement, topology changes in unpredictable manner.
- Limited Energy: Every operation performed by the mobile devices consumes energy so it limits the processing power of mobile devices.
- Multihop Routing: Each node in a MANET act as a router and forward packet to the destination node or an intermediate node within the communication range towards destination.
- Bandwidth Constraint: Wireless links have lower capacity. Throughput of wireless communication is less because of the effect of multiple access, fading, noise, interference conditions. Because of this, congestions become a bottleneck in bandwidth utilization.

There are various protocols to facilitate successful communication in a decentralized and a dynamic environment of MANET. But among them AODV is mostly used protocol because it enables dynamic, self-starting, multi-hop routing between participating nodes willing to establish mobile ad hoc network. Routes to new destination nodes can be established on demand. However, AODV is vulnerable to various security attacks. One of the popular attacks on AODV is the black hole attack.

In black hole attack, a malicious node obtains route from source to destination falsely and drops all received packets without forwarding it resulting in Denial of Service attack.

II. AODV ROUTING PROTOCOL UNDER BLACK HOLE ATTACK

AODV is a reactive on-demand and distance-vector routing protocol. The routing in AODV is carried out in two phases:

1. Route discovery
2. Route maintenance

Whenever a source node wants to send data to destination node whose path is not present in its routing table, route discovery process is initiated by broadcasting a RREQ (Route request) packet. Neighbor nodes check if it is destination or have a route to destination in their routing table. In that case, it will send a RREP (Route reply) packet on the reverse path as shown in the Fig 1.

If path is not available, it will increment the hop count by one and further broadcasts a RREQ. During the transmission of data if any node identifies route break, it will send a RERR (Route Error) message. Freshness of the path

is measured by destination sequence number. Source node choose path with a higher destination sequence number and low hop count.

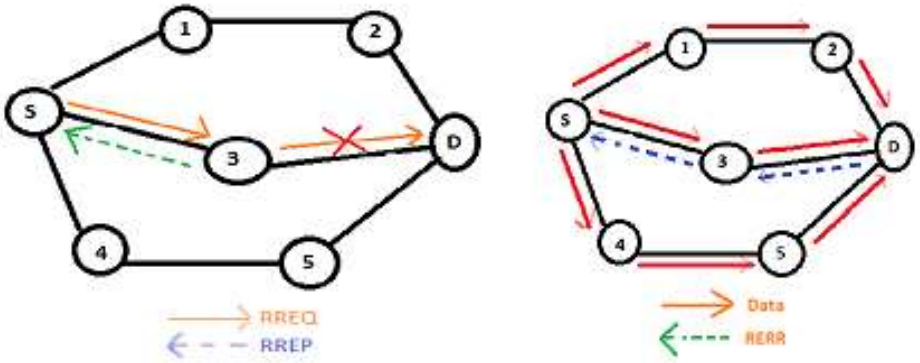


Figure 1. Route Discovery & Maintenance Process of AODV [17]

In the Black hole attack, malicious node receives a RREQ packet and sends a RREP with a higher destination sequence number. Source node reacts to the RREP with higher sequence number and considers that route as fresh and starts sending data packets. The malicious node does not forward the data packets and drops them reducing packet delivery ratio and increasing the network congestion.

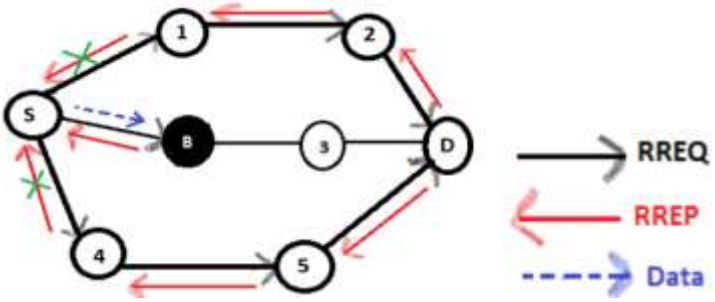


Figure 2. Black Hole Attack in AODV [17]

In the Fig. 2, Black colored Node B (Malicious node) falsely sends RREP to source node S with a higher sequence number. As source node does not have any prior information about destination in its table, it starts sending data to node B which further drops the packets.

III. LITERATURE SURVEY

S. No.	Research Paper Title	Method	Pros	Cons
1.	Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks [5,6]	DRI and Cross Checking	A higher throughput performance almost 50% than AODV	5-8% more communication overhead of route request
2.	DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV based MANET [8]	Sequence number compared with Threshold value and ALARM packet to neighbor nodes for isolating black hole node	The PDR is improved by 80-85% than AODV when under black hole attack	May mistakenly block some non-malicious node due to its high Seq_no also little bit higher routing overhead and end-to-end delay
3.	Implementation of Routing Security Aspects in AODV [9]	Only DN allowed to RREP, ALARM packet for isolation of black hole node	PDR of SAODV is more immune that AODV	Takes 1% extra time in transmitting data packets compared to AODV
4.	Secure Routing with the AODV Protocol [7]	Cryptographic mechanism based solution. Encryption using symmetric key	Higher throughput and PDR compared to AODV	Higher routing overhead due to point to point encryption/ decryption
5.	Securing AODV: The A-SAODV Secure Routing Prototype [10]	Digital Signature and adaptive reply decision	Some enhancements in SAODV to improve the performance	Increased overhead and complexity
6.	Secure AODV protocol to	uses the ratio of the	PDR increases by	Well-connected nodes

	mitigate Black hole attack in Mobile Ad hoc Networks [12]	number of route request on number of route reply forwarded by node in the network to detect a black hole attack	78.6%	may falsely understood as malicious node, Time consuming technique
7.	Securing Routing Table Update in AODV Routing Protocol [11]	Uses Enhanced Route discovery AODV (ERDA) to control the update of the routing table.	Isolates the attacker at initial stage, PDR increases up to 77%	Minimal overhead, Delay in attacker detection

In all the above proposed solutions, throughput and PDR increases but at the cost of higher overhead. In the next section, I have proposed a hybrid solution combining [11] & [12] in which PDR ratio raises up to 80% without high cost or overhead.

IV. PROPOSED SOLUTION

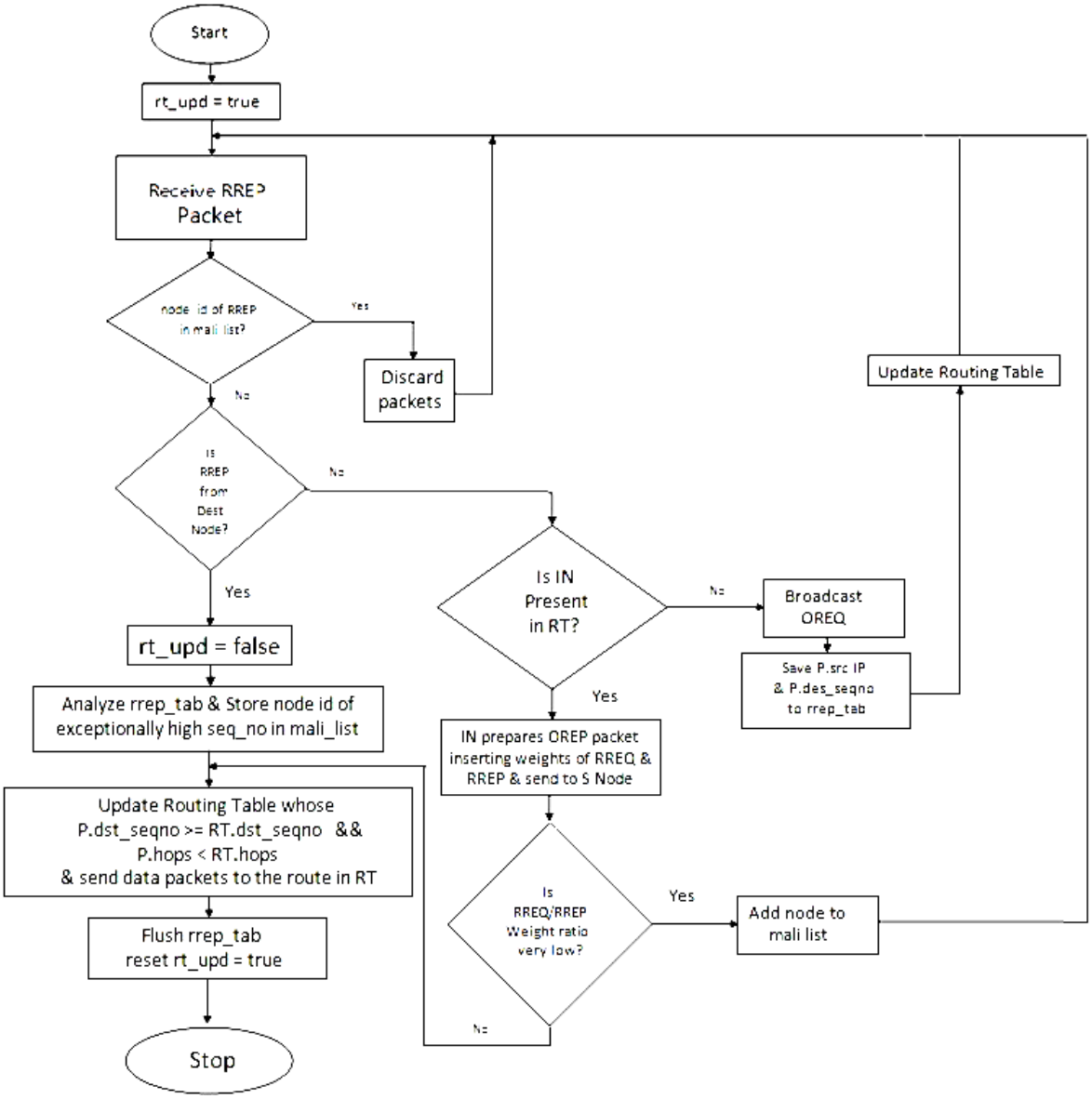


Figure 3. Proposed Solution

In AODV protocol under black hole attack, malicious node send false RREP packet as a response to RREQ packet to attract traffic towards it. Black hole node sends RREP even if it does not have the path towards the destination requested by the source of RREQ. It does not broadcast RREQ, instead sends RREP without checking its routing table. So for the malicious node the ratio of number of RREQs transmitted to the number of RREPs transmitted is very less. This fact is useful to detect the black hole attack. For doing so, two extra fields will be used in the proposed solution - request weight and reply weight. Request weight in routing table indicates the number of RREQs that are forwarded by the corresponding node. Similarly Reply weight indicates the number of RREPs forwarded.

The only problem with the above proposed solution is it can falsely declare the silent node as a malicious node because the "RREQ and RREP Weights Ratio" of any silent node will always be near to zero because the silent node rarely generates any RREQ but it can have high number of RREP. The solution of above problem is to check the *Destination_Sequence_Number (DSN)* of particular node. Researches show that the DSN of any malicious node tends to be abnormally higher than other intermediate nodes in the N/W. So the DSN can be compared with DSN of other nodes and analyzed through heuristics for its abnormality. If the node is a silent node then its DSN will be normal compared to other nodes but if the node is malicious and is trying to perform black hole attack then its DSN will be very large compared to DSN of other nodes. So such node can be black listed out as a malicious node.

To do so, in our proposed method, an additional parameter called *rt_upd* is included. This parameter can receive either true or false value. By default, the value is set to true which means the routing table is allowed to be updated and it is not necessary from the first RREP message received by the node. Multiple RREPs are collected rather than the single RREP when the *rt_upd* is true. The RREPs will be stored in a new table called *rrep_tbl.* Once the updating receives the RREP message from the destination node D, the *rt_upd* parameter value is then set to false. Any RREP message that comes after this point will be denied from updating the routing table until the process of detecting malicious node is completed. The source node has already saved all the coming RREP in *rrep_tab* table. Subsequently, the source node analyses all the stored RREPs from *rrep_tab* table, and discard the RREP having presumably very high destination sequence number. As before, the node that sent this RREP is suspected to be the malicious node. Once, such malicious node is identified, this solution selects a reply having highest destination sequence number from *rrep_tab* table. The malicious nodes are stored in table *mali_list* to inform the node to isolate those listed nodes from participating in the route discovery updates. Thus, any control messages (e.g. RREP or RREQ) that come from those listed nodes will be discarded by the node. In order to ensure that this process does not consume memory, the *rrep_tab* table will be flushed once the process of identifying malicious node is completed and the *rt_upd* parameter value again is set back to true. By the above discussed techniques, we can eliminate the malicious node very effectively with no false alarm for silent nodes.

IV. PERFORMANCE ANALYSIS

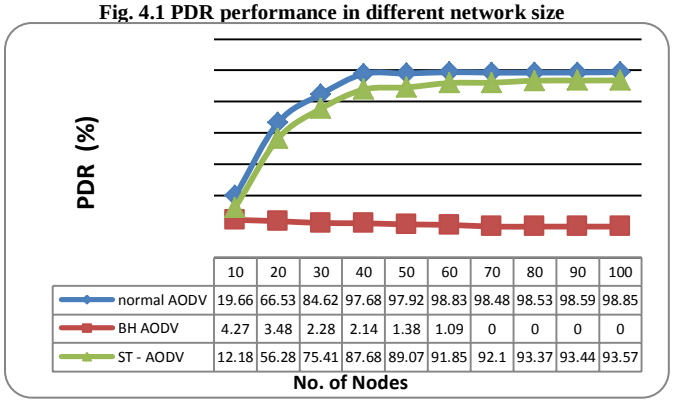
Various Performance metrics like PDR, NRL and End-to-End Delay are calculated against varying number of nodes and varying mobility speeds of the nodes in the N/W under scenarios without attack and with Black hole attack. For the simulations, we use NS-2 (v-2.35) network simulator. Below is the specification table for simulation.

Table 1. Simulation Parameters

Parameter	Value
Simulator	NS-2 Version 2.35
Simulation Time	100 s
Number of Nodes	10 to 100
Routing Protocol	AODV
Traffic Model	CBR
Packet Size	512 bytes
Pause Time	2 s
Mobility	10 to 70m/s
Terrain	200m x 200m
Transmission Range	50m
Number of Malicious Nodes	1
Name of Attack	Black Hole

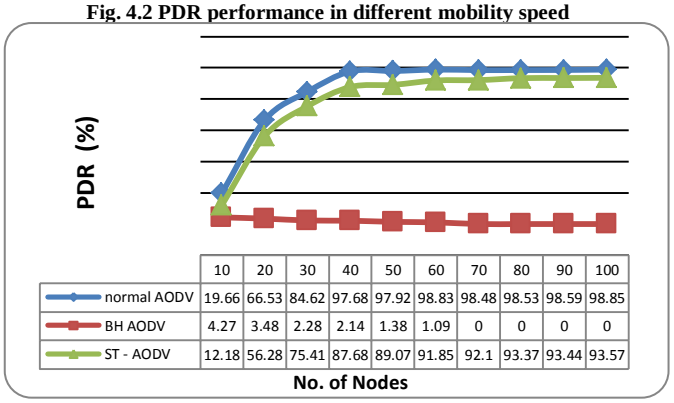
Table 2. Simulation Results

Fig. 4.1 PDR performance in different network size



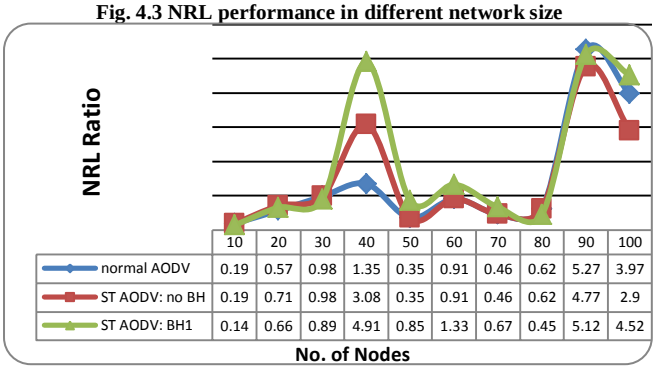
	10	20	30	40	50	60	70	80	90	100
normal AODV	19.66	66.53	84.62	97.68	97.92	98.83	98.48	98.53	98.59	98.85
BH AODV	4.27	3.48	2.28	2.14	1.38	1.09	0	0	0	0
ST - AODV	12.18	56.28	75.41	87.68	89.07	91.85	92.1	93.37	93.44	93.57

Fig. 4.2 PDR performance in different mobility speed



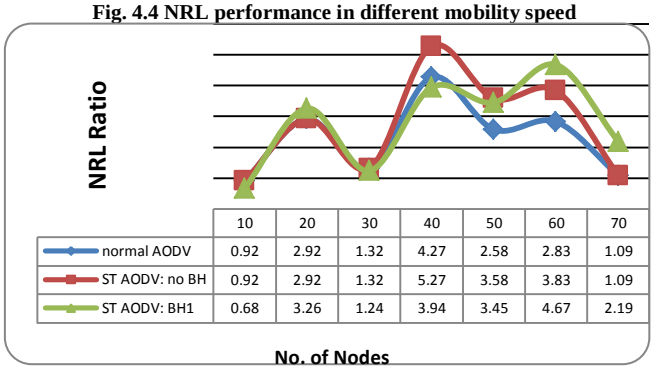
	10	20	30	40	50	60	70	80	90	100
normal AODV	19.66	66.53	84.62	97.68	97.92	98.83	98.48	98.53	98.59	98.85
BH AODV	4.27	3.48	2.28	2.14	1.38	1.09	0	0	0	0
ST - AODV	12.18	56.28	75.41	87.68	89.07	91.85	92.1	93.37	93.44	93.57

Fig. 4.3 NRL performance in different network size



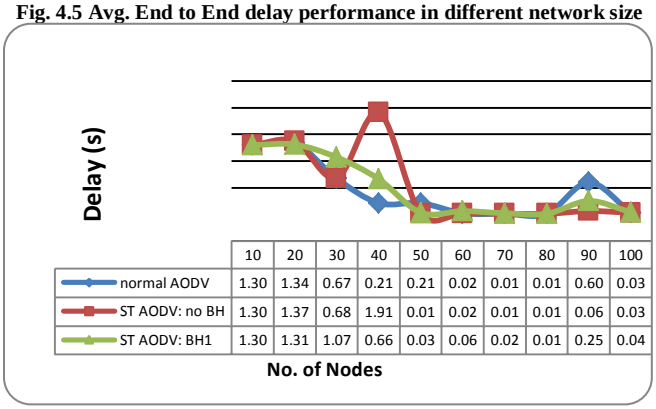
	10	20	30	40	50	60	70	80	90	100
normal AODV	0.19	0.57	0.98	1.35	0.35	0.91	0.46	0.62	5.27	3.97
ST AODV: no BH	0.19	0.71	0.98	3.08	0.35	0.91	0.46	0.62	4.77	2.9
ST AODV: BH1	0.14	0.66	0.89	4.91	0.85	1.33	0.67	0.45	5.12	4.52

Fig. 4.4 NRL performance in different mobility speed



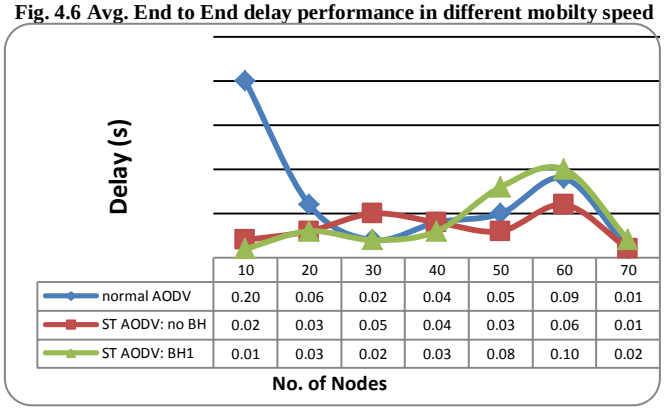
	10	20	30	40	50	60	70
normal AODV	0.92	2.92	1.32	4.27	2.58	2.83	1.09
ST AODV: no BH	0.92	2.92	1.32	5.27	3.58	3.83	1.09
ST AODV: BH1	0.68	3.26	1.24	3.94	3.45	4.67	2.19

Fig. 4.5 Avg. End to End delay performance in different network size



	10	20	30	40	50	60	70	80	90	100
normal AODV	1.30	1.34	0.67	0.21	0.21	0.02	0.01	0.01	0.60	0.03
ST AODV: no BH	1.30	1.37	0.68	1.91	0.01	0.02	0.01	0.01	0.06	0.03
ST AODV: BH1	1.30	1.31	1.07	0.66	0.03	0.06	0.02	0.01	0.25	0.04

Fig. 4.6 Avg. End to End delay performance in different mobilty speed



	10	20	30	40	50	60	70
normal AODV	0.20	0.06	0.02	0.04	0.05	0.09	0.01
ST AODV: no BH	0.02	0.03	0.05	0.04	0.03	0.06	0.01
ST AODV: BH1	0.01	0.03	0.02	0.03	0.08	0.10	0.02

V. CONCLUSION AND FUTURE WORK

The vulnerabilities of AODV protocol make it weak entity in terms of security against various attacks especially for Black hole attack. Our proposed hybridized solution opts to secure AODV against such attack. The RREQ/RREP Weights Ratio work very well to detect and prevent the Black hole attack but it is susceptible to give false alarm for silent nodes in the MANET. And to solve the problem of silent node we merge the technique of multiple RREPs with previous technique that efficiently removes the malicious node out of the N/W with no false alarms. Due to the mitigation of Black hole attack it can be assumed that the metrics like PDR and throughput may result higher but the average end-to-end delay can increase little bit in result due to some computational overheads. The simulation results are analyzed for sample topology having single black hole node which generates up to 80% higher PDR compared to AODV.

For the future work, topology with multiple black hole nodes will be created and will collect and compare the simulation results of various metrics of an AODV protocol like NRL, PDR and Average End-to-End Delay under various scenario like performance of AODV in absence of malicious node, in presence of malicious node and an enhanced AODV with our proposed solution.

REFERENCES

[1] IEEE Standard 802.11-1999, Institute of Electrical and Electronics Engineers, "Standard for Local and metropolitan area networks - specific requirements - part 11: Wireless LAN Medium Access Control and Physical Layer specifications", 1999.

[2] IEEE Standard 802.16-2004, Institute of Electrical and Electronics Engineers, "Standard for Local and metropolitan area networks - specific requirements- part 16: Air Interface for Fixed Broadband Wireless Access Systems", October 2004.

[3] E. M. Royer and C.-K. Toh. A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. IEEE Personal Communications Magazine,April 1999, pp. 46-55.

[4] Asad Amir Pirzada and Chris McDonald, "Secure Routing with the AODV Protocol," Asia-Pacific IEEE Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.

[5] Ramaswamy S, Fu H, Sreekantaradhya M, Dixon J, Nygard K., "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," International Conference on Wireless Networks, Las Vegas, Nevada, USA, 23-26 June 2003.

[6] Weerasinghe H, Fu H., "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation," Future Generation Communication and Networking, Jeju-Island, Korea, 6-8 December 2007.

[7] Asad Amir Pirzada and Chris McDonald, "Secure Routing with the AODV Protocol," Asia-Pacific IEEE Conference on Communications, Perth, Western Australia, 3 - 5 October 2005.
[8] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System AgainstBlackhole Attack in AODV based MANET," International Journal of Computer Science Issues, Vol.2, 2009.
[9] Suman Deswal and Sukhbir Singh, "Implementation of Routing Security Aspects in AODV," International Journal of Computer Theory and Engineering, Vol. 2, No. 1, pp. 135-138, 2010.
[10] Davide Cerri, Alessandro Ghioni, "Securing AODV: The A-SAODV Secure Routing Protocol," IEEE Communications Magazine, Vol. 46, No. 2, pp. 120-125, 2008.
[11] K.A. Jalil, Z. Ahmad and J. A. Manan "Securing Routing Table Update in AODV Routing Protocol," IEEE Conference on Open Systems, Langkawi, pp. 116-121, 2011.
[12] Rajesh Yerneni and A.K. Sarje "Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks," IEEE Conference on Computing Communication and Networking Technologies, Coimbatore, pp. 248-252, 2012.
[13] A.MenakaPushpa, "Trust Based Secure Routing in AODV Routing Protocol", IEEE Conference on Internet Multimedia Services Architecture and Applications, Bangalore, 2009.
[14] M. Jarrett and P. Ward, "Trusted Computing for Protecting Ad-hoc Routing", IEEE Conference on Communication Networks and Services Research Conference, 2006.
[15] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communication Surveys, Vol. 14, No. 2, 2012.
[16] N. Mistry, D. CcJinwala, M.Zaveri, "Improving AODV Protocol against Blackhole Attacks", proceedings the International Multi Conference of Engineers and Computer Scientists, Vol.2, Hong Kong, 2010.
[17] Teerawat Issariyakul, Ekram Hossain, "Introduction to Network Simulator NS2", Springer 2008.