International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-4 Issue-3, February 2015

# Proposing AODVSC Protocol to Detect Black Hole Attacks in Mobile Ad-hoc Network

**Luong Thai Ngoc, Vo Thanh Tu**

***Abstract — Mobile Ad-hoc Network (MANET) is a kind of wireless network, which has no infrastructure and is a self configuring wireless network of mobile nodes, each node on the MANET acts like a router which forwards the packets. Due to these properties, MANET is vulnerable to attacks, routing attack is the most common one. The black hole attack is a kind of routing attack made by a malicious node on MANET. This article proposes AODVSC improved from AODV protocol which uses SC (Safe Cycle) solution to detect black hole attacks. The SC solution uses the "distance" from the current node to all neighboring nodes based on SN (sequence number) values. The simulated installation and performance evaluation of AODVSC and AODV protocols in the normal network environment where there are black hole node attacks on the network simulator NS2 was also presented to evaluation improved protocol.***

***Index Terms — AODV, AODVSC, black hole, detect black hole attacks, mobile ad hoc network, routing protocols.***

## I. INTRODUCTION

MANET is flexible, is a set of independent mobiles, nodes communicating with each other in a dynamic topology which can easily join and leave to the network. The mobile node can be PDA, laptop, mobile phone and so on. The connectivity of mobile nodes via wireless channel is used hop by hop routing. So, the nodes may be router or host [5]. Due to its characteristics, MANET is unprotected to various kinds of attacks, such as: Black hole [4], gray hole [16], worm hole [7], sink hole [10], flooding [13].

The routing protocols for MANET are classified as proactive, reactive and hybrid protocols [2]. AODV is reactive routing protocol because it initiates route discovery only when it is needed. It is based on source routing, it maintains a route cache at each node and the route is maintained on a node until it is required or the destination is unreachable [11].

The possible type of attacks on MANET are active and passive attacks. Monitoring and listing to the communication channel by unauthorized nodes is categorized as a passive attack. Whereas, active attacks are those in which a malicious node monitors, listens, modifies the packets or add new packets on the network [15]. The black hole is an active attack, is performed on the network layer where a malicious node advertises itself as having the shortest path to all nodes in the system by sending fake route reply (RREP) packets. By doing this, the malicious node can deprive the traffic from the source node and drops the packets later [4].

The limited research of this paper is to show the black hole attack behavior and its impact. Thence, propose AODVSC protocol to detect black hole attacks using ns2 [18] to simulate. The rest of the paper is organized as follows, Section 2 reviews the related works done to detect black hole attacks on MANET, Section 3 describes how to black hole attack AODV protocol, Section 4 proposes the AODVSC protocol to detect black hole attacks, Section 5 is a simulation and analysis of black hole attacks with AODV and AODVSC, and Section 6 shows the conclusion and future works.

## II. RELATED WORKS

There are various solutions are proposed to detect and prevent the black hole attacks. Some of these research papers were reviewed in this section.

In [15], Semih D proposes idsAODV protocol to prevent black hole attacks, the main idea is that source node removes the first RREP packet and accepts the second packet to define route. Thus, source node discovers a new route with the cost which is not the best, sometimes this route has the next hop is malicious node because it does not detect fake RREP packet which is used to attack routing table.

In [14], Satoshi K and collaborators propose the solution to detect black hole attacks based on dynamic learning algorithm. This algorithm uses threshold to detect black hole attacks, this value is counted after interval time based on data set training. In [12], Raj P.N and Swadas P.B propose DPRAODV protocol which can *detect, prevent and reactive* when black hole attacks appeared. The main idea is to add a module to check reliable of RREP packets into source node. That is a comparison of the SN value with a dynamic updated threshold. If the sequence number value is found to be higher than the threshold value, the destination node is suspected to be malicious and it adds the node to the black list.

In [8], Mohammad A.O and collaborators propose AODV$_R$ has introduced several modules such as Threshold Tester, RREP sequence number Tester, Blacklist Tester, Extractor, Packet Classifier and ALARM broadcaster. In this method, the router calculates the range of the accepted sequence numbers and gives the threshold value. If any node exceeds the threshold values for several times, it is identified as black hole node. There are several intelligible researches has been carried out based to secure routing in MANET. SAODV [6] protocol is a security extension of AODV protocol, based on public key cryptography. Hash chains are used in this protocol to authenticate the hop count. A-SAODV [3] protocol has proposed a mechanism based on SAODV for improving the performance of SAODV.

**Manuscript published on 28 February 2015.**
* Correspondence Author (s)
**Luong Thai Ngoc***, Faculty of Mathematics and Information Technology Teacher Education, Dong Thap University, Dong Thap Province, Viet Nam.
**Vo Thanh Tu**, Faculty of Information Technology, Hue University of Science, Hue City, Viet Nam.

In [1], a bit of modification has been applied to A-SAODV for increasing its performance. In [9], Mohan K.S.B and collaborators propose cryptographic approach to overcome black hole attack in MANETS. In [17], Suketu D.N and collaborators propose Sec.AODV for MANETs using MD5 with cryptography. This solution group has the benefit that the security is very good. However, the average end-to-end delay of system is increase and how to manage and allocate keys is a difficult problem.

## III. Black Hole Attacks Aodv Protocol In Manet

The goal of the malicious node in this attack is to drop all packets that are directed to it, instead of forwarding them as intended. It uses fake RREP or route request (RREQ) packets in order to advertise itself as having the shortest route to the destination node [4]. In this way the malicious node will always have availability of routes while replying to the route request and hence intercept the data packets.

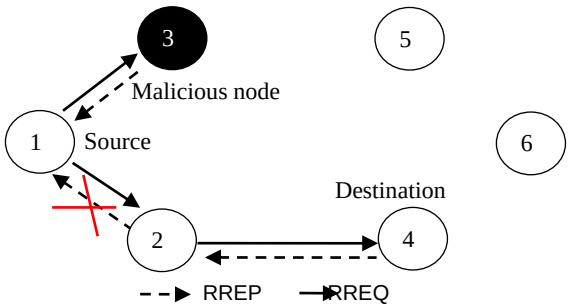


**Figure 1. Topology with malicious node**

In topology network (Fig 1), source node (1) discovers a new route to destination node (4), it broadcasts RREQ packets to all neighbor nodes. The direction of RREQ packet is (1)→(2)→(4) and (1) →(3). When malicious node (3) receives RREQ packets which reply a fake RREP packet (Table 1) to back source node (1) in order to advertise itself as having the shortest route to the destination node, this fake packet's HC value = 1 and DSN value is very large, this article uses DSN = 4294967295 because DSN type size is unsigned integer in NS-2. Source node (1) received two RREP packets from node (3) and node (2). In that the first packet has cost which is the best, thus routing table of source node (1) has route information to node (4) with next hop is node (3). Routing information of source node (Table 2) shows that node (1) wants to send data to node (4) which must send to node (3) with the cost is 1. The result is the malicious node (3) receives all packets from node (1) and it drops all.

**Table 1. The fake RREP packet's information**

```
sendReply (rq->rq_src, 1,
           index, 4294967295,
           MY_ROUTE_TIMEOUT,
           rq->rq_timestamp);
```

**Table 2. Routing table in source node**

| Source | Destination | Next hop | SN | HC |
|---|---|---|---|---|
| 1 | 4 | 3 | 4294967295 | 1 |

## IV. Propose Aodvsc Protocol

This article proposes a solution to detect black hole attacks based on SC (Fig 2) at every node to detect fake RREP packets. Thus, each node can prevent malicious nodes appear in system.

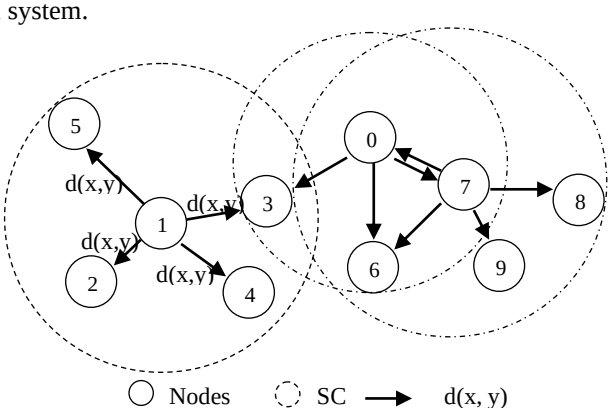


**Figure 2. Safe Cycle on node 0, 1 and 7**

See topology network (Fig 2), supposing that O is Safe Cycle at each of node, O(i) is Safe Cycle of node (i). We build O(i) which is cycle with center is node (i), radius $R_i$ *is* defined as formula 1 and radius *d* is defined as formula 2. In that n is the total of nodes in system and m is the total neighbors of node (i).

$$R_i = \max(d(node(i), node(j)); \forall i = \overline{1..n}; \forall j = \overline{1..m} \quad (1)$$

$$d(x, y) = \begin{cases} 0 & ; if\ x.SN > y.SN \\ y.SN - x.SN & ; else \end{cases} \quad (2)$$

In the figure 3 shows algorithm scheme for update Safe Cycle at node (S), the algorithm complex is O(n).

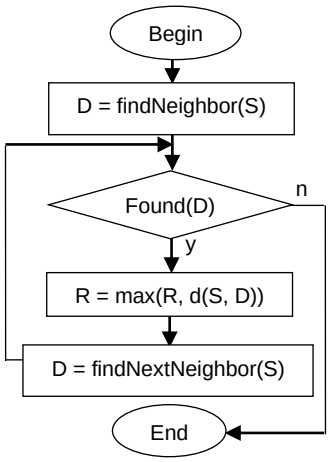


**Figure 3. Algorithm for update SC at node (S)**

In original AODV, the source node accepts all RREP packets to define route in its routing table. Our improve solution is add module into source node to check validation of RREP packets (Fig 4). The kc value is computed as formula 2 when node receive the RREP packet from neighbors. The black hole attacks appear if kc is larger than R of node's SC, then the routing table of node is not updated, the algorithm complex is O(1).


Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

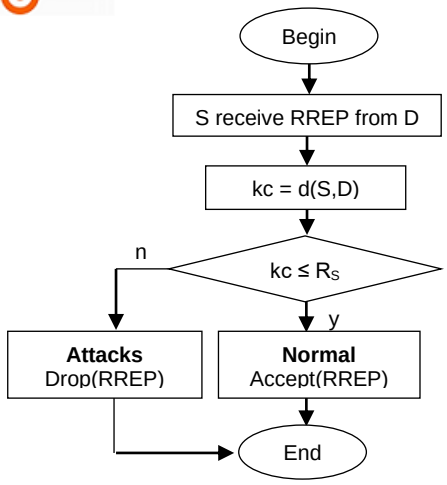


**Figure 4. Module to detect black hole attacks**

## V. THE SIMULATION RESULTS

For simulation, the article has used ns-2.35 network simulator. Mobility scenarios are generated by using a Random way point model [19] with 50 nodes moving in a terrain area of 900m x 900m. Various network contexts are considered to measure the performance of a protocol. These contexts are created by varying the following parameters in the simulation, that is the number of malicious nodes and maximum mobility (Summarized in Table 3).

**Table 3. Simulation parameters**

| Parameters | Values |
|---|---|
| Simulator area | 900m x 900m |
| Network topology | Random Way Point |
| Simulation time | 1000s |
| Number of nodes | 50 (node) |
| Pause time | 4 (s) |
| Traffic Model | CBR |
| Maximum connection | 5 UDP |
| Packet size | 512 (bytes) |
| Routing protocols | AODV, AODVSC |
| Maximum mobility | 2, 4, 6, 8, 10, 12, 14, 16, 18, 20 (m/s) |
| Number of malicious | 0: Normal and 1: Attacks |

The simulation is done to analyze the performance of the network's various parameters. The metrics used to evaluate the performance are given below:

- Packet Delivery Ratio (PDR): The ratio of the data delivered to the destination to the data sent out by the source.
- Total of Dropped Packets (TDP): The total of packet dropped due to black hole attacks.
- Average End-to-end delay (AED): The difference in the time it takes for a sent packet to reach the destination.

The article evaluates performance of AODV and AODVSC protocols with 40 simulation scenario in normal environment or with black hole attacks. The simulation result shows in Table 4, the performance charts are showed in Figure 5, 6, 7.

**Table 4. The simulation results**

| Speeds (m/s) | | Normal | | Attacks | |
|---|---|---|---|---|---|
| | | AODVSC | AODV | AODVSC | AODV |
| Packet delivery ratio | 2 | 92.73% | 94.95% | 93.12% | 12.73% |
| | 4 | 88.21% | 92.55% | 90.78% | 12.54% |
| | 6 | 88.75% | 88.56% | 84.69% | 7.93% |
| | 8 | 87.79% | 89.79% | 88.61% | 11.18% |
| | 10 | 85.16% | 86.91% | 86.14% | 14.67% |
| | 12 | 85.53% | 86.50% | 84.48% | 17.48% |
| | 14 | 84.56% | 85.52% | 83.38% | 11.93% |
| | 16 | 82.73% | 85.58% | 82.95% | 17.31% |
| | 18 | 82.86% | 84.03% | 83.54% | 15.64% |
| | 20 | 79.75% | 82.83% | 79.55% | 15.04% |
| Total of dropped packets | 2 | 6.74% | 4.99% | 6.64% | 86.26% |
| | 4 | 11.42% | 7.09% | 8.62% | 87.33% |
| | 6 | 11.08% | 11.36% | 15.05% | 91.80% |
| | 8 | 11.99% | 10.08% | 11.22% | 88.51% |
| | 10 | 14.33% | 12.76% | 13.59% | 85.11% |
| | 12 | 14.33% | 13.03% | 14.97% | 81.88% |
| | 14 | 15.17% | 14.19% | 16.22% | 87.71% |
| | 16 | 16.85% | 14.03% | 16.57% | 82.45% |
| | 18 | 16.75% | 15.64% | 16.19% | 83.89% |
| | 20 | 19.59% | 16.71% | 19.66% | 84.61% |
| Average end-to-end delay | 2 | 0.037s | 0.025s | 0.068s | 0.066s |
| | 4 | 0.054s | 0.033s | 0.183s | 0.073s |
| | 6 | 0.086s | 0.050s | 0.079s | 0.038s |
| | 8 | 0.123s | 0.036s | 0.121s | 0.204s |
| | 10 | 0.098s | 0.153s | 0.162s | 0.095s |
| | 12 | 0.219s | 0.131s | 0.228s | 0.320s |
| | 14 | 0.141s | 0.060s | 0.147s | 0.060s |
| | 16 | 0.146s | 0.090s | 0.175s | 0.191s |
| | 18 | 0.220s | 0.222s | 0.212s | 0.257s |
| | 20 | 0.192s | 0.160s | 0.154s | 0.143s |

Figure 5 shows the effect to the PDR measured for the AODV and AODVSC protocols when the node mobility is increased. The result shows both the cases, with the black hole attack and without the black hole attack. It is measured that the DPR of AODVSC is equivalent with AODV protocol in normal environment. The DPR of AODV is dramatically decreases when there is a malicious node in the network. For example, the DPR is 94.95% when there is no effect of Black hole attack and when the node is moving at the speed 2 m/s. However, due to effect of the black hole attack the DPR decreases down to 12.73% because the large numbers packets are dropped (Fig 6b) by the black hole attacks.


Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

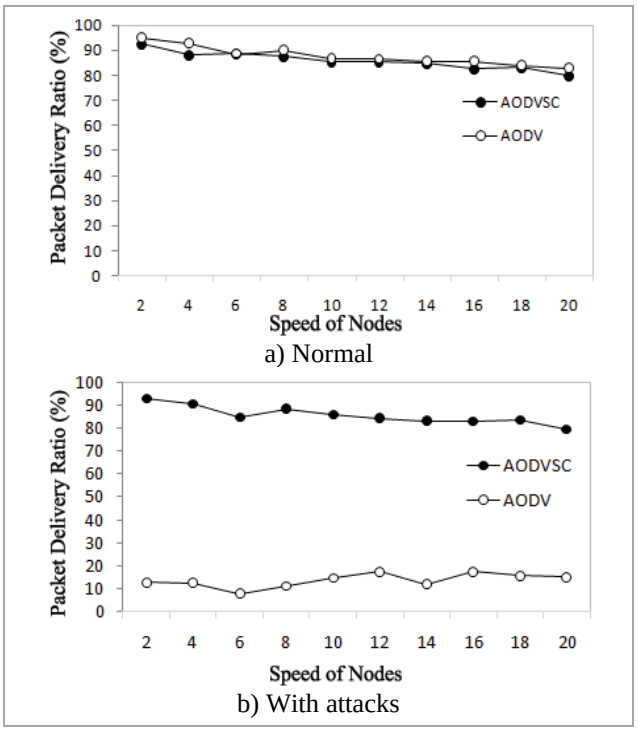


**Figure 5. The chart of packet delivery ratio**

Figure 6a shows the both protocols have the dropped packets is very low in normal environment and increase when nodes move with high speeds. However, in the black hole attacks environment, the packets are dropped in AODV protocol is very large (≥82.45%), this effects the PDR of AODV protocol. In figure 6b shows the packets are dropped of AODVSC protocol is very low (≤19.66%), this shows the improved solution can successfully prevent black hole attacks.

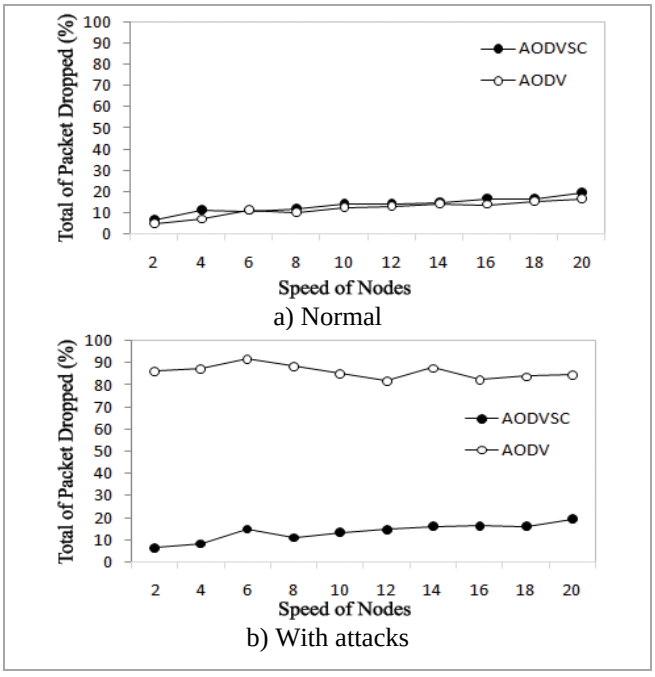


**Figure 6. The chart of dropped packets**

Figure 7a shows the average end to end delay (AED) increases when all nodes move with high speeds in all scenarios. There is difference in the AED of the both AODV and AODVSC protocols but it is acceptable. With black hole attacks, the AED will increase if malicious node stays far from source, else it decreases. Figure 7b shows the AED of AODVSC protocol is stable because AODVSC prevents black hole attacks successfully.

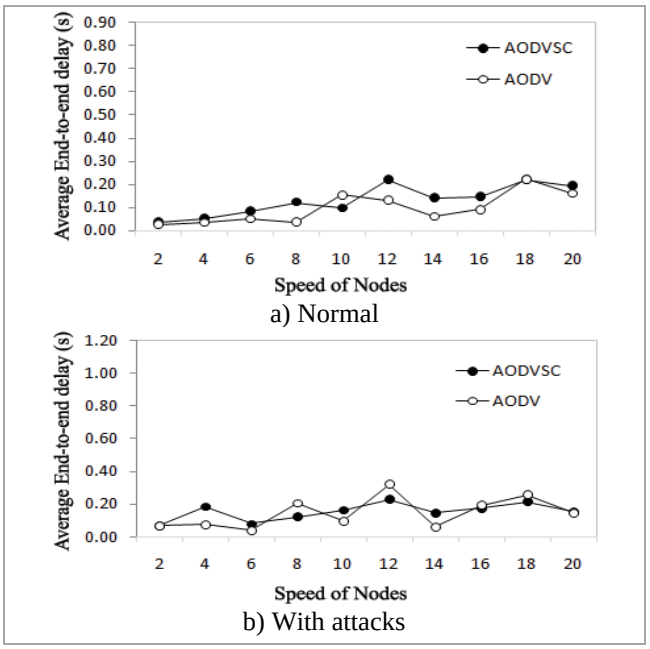


**Figure 7. The chart of average end-to-end delay**

## VI. CONCLUSION

In this article, a simple solution for detecting the black hole attacks in AODV is proposed. The proposed algorithm can be applied to detect and prevent the malicious node and to gain the secured route from source to destination in the MANET. The comparison of improved AODVSC and AODV is done using NS-2.35. The performance metrics such as packet delivery ratio, total of dropped packets, average end to end delay has been evaluated and analyzed with the variable node mobility, and a number of malicious nodes. The proposed solution is effective against black hole attacks and it has high packet delivery ratio. However, the end to end delay of AODVSC is gradually increased than the original AODV protocol in all scenarios without attacks. In the future work, we are going to improve the AODVSC protocol to change operation state automatically such as AODV protocol in normal environment, and prevent state in where there are black hole attacks appear.

## REFERENCES

[1] Alekha Kumar Mishra, Bibhu Dutta Sahoo, "A modified Adaptive SAODV prototype for perfor-mance enhancement in MANET", *IJ-CA-ETS, Vol 1, Issue 2*, 2010, pp. 443-447.
[2] Anu Bala, Raj Kumari and Jagpreet Singh, "Investigation of Blackhole Attack on AODV in MANET", *journal of emerging technologies in web intelligence, vol. 2, no. 2*, 2010, pp. 96-100
[3] Cerri D, Ghioni A, "Securing AODV: The A-SAODV Secure Routing Prototype", *IEEE Com-munication Magazine*, 2008, pp. 120-125.
[4] Ei Ei Khin, and Thandar Phyu, "Mitigating Scheme for Black Hole Attack in AODV Routing Protocol", *ICAET, 2014*, pp. 105-109.
[5] Irshad Ullah, Shoaib Ur Rehman, *Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols*, School of Computing Blekinge Institute of Technology, MA, 2010.
[6] Manel Guerrero-Zapata, *Secure Ad hoc On-Demand Distance Vector (SAODV) Routing*, guerrero/draft-guerrero-manet-saodv-05.txt, 2005.
[7] Mahajan V, Natu M and Adarshpal Sethi, "Analysis of wormhole Intrusion Attacks In MANETS", *IEEE, 978-1-4244-2677*, 2008.


*Published By:*
*Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)*

[8] Mohammad A.O, Shahnewaz A.F, Abu H, Tanay K.R, "AODV robust ($AODV_R$): an analytic approach to shield ad-hoc networks from black holes", *International Journal of Advanced Computer Sciences and Applications, vol. 2, issue 8*, 2011, pp. 97-102.
[9] Mohan K.S.B, Nirmal K.S.B, "Cryptographic Approach to Overcome Black Hole Attack in MANETS", *Vol.2 Issue 3*, 2013, pp. 86-92.
[10] Mohammed A.H, Francis S.D, "Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET", *IJERA, Vol. 3, Issue 2*, 2013, pp. 1737-1741.
[11] Perkins C, Royer E. B and Das S, *Ad hoc on-demand distance vector (aodv) routing*, RFC: 3561, Nokia Research Center, 2003.
[12] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET", *International Journal of Computer Science, Vol.2*, 2009, pp. 54–59.
[13] Ruchita Meher, Seema Ladhe, "Review Paper on Flooding Attack in MANET", *IJERA, Vol. 4, Issue 1( Version 2)*, 2014, pp. 39-46
[14] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, etc, "Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security, Vol.5, No.3*, 2007, pp. 338–346.
[15] Semih Dokurer, *Simulation of black hole attack in wireless ad-hoc networks*, Atılım University, MA, 2006.
[16] Shanmuganathan V, Anand T, "A Survey on Gray Hole Attack in MANET", *International Journal of Computer Networks and Wireless Communicat-ions, Vol.2, No.6*, 2012, pp. 647-650.
[17] Suketu D.N, Ravindra K.G, "Sec.AODV for MANETs using MD5 with Cryptography", *Int. J. Comp. Tech, Vol.2, No.4*, 2011, 873-878.
[18] Teerawat Issariyakul, Ekram Hossain, *Introduc-tion to Network Simulator NS2*, Springer Science + Business Media, 2009.
[19] Yoon J, Liu M, Noble B, Random Waypoint Considered Harmful, *0-7803-7753-2/03, IEEE INFOCOM*, 2003.