# A Collusion Attack Against OLSR-based Mobile Ad Hoc Networks

Bounpadith Kannhavong, Hidehisa Nakayama,
Nei Kato, and Yoshiaki Nemoto
Graduate School of Information Sciences
Tohoku University
Sendai-shi, Miyagi, 980–8579, Japan
tansekei@it.ecei.tohoku.ac.jp

Abbas Jamalipour
School of Electrical and Information Engineering
The University of Sydney
Sydney NSW 2006, Australia

*Abstract*— **Rapid advances in wireless networking technologies have made it possible to construct a Mobile Ad hoc Network (MANET) which can be applied in infrastructureless situations. However, due to their inherent characteristics, MANETs are vulnerable to various kinds of attacks which aim at disrupting their routing operations. To develop a strong security scheme to protect against these attacks it is necessary to understand the possible form of attacks that may be launched. Recently, researchers have proposed and investigated several possible attacks against MANET. However, there are still unanticipated or sophisticated attacks that have not been well studied. In this paper, we present a collusion attack model against Optimized Link State Routing (OLSR) protocol which is one of the four standard routing protocols for MANETs. After analyzed the attack in detail and demonstrated the feasibility of the attack through simulations, we present a technique to detect the attack by utilizing information of two hops neighbors.**

**Keyword:** ***MANET, OLSR, Collusion Attack***

## I. Introduction

Along with the proliferation of mobile computing devices and advances in wireless communication technologies, Mobile Ad hoc Networks are receiving more and more attention from the networking research and industry community. A Mobile Ad hoc Network (MANET) is a collection of mobile nodes interconnected by wireless links without the aid of any fixed infrastructure or centralized access point such as a base station. In MANET, each node acts both as a host and as a router to forward messages for other nodes that are not within the same radio range. The nodes are free to move and form an arbitrary topology. MANET can be established in situation where no infrastructure exists, or when deployment of infrastructure is inconvenient or expensive. This inherent flexibility makes it attractive for applications such as emergency operation, disaster recovery, maritime communication, military operation, one-off meeting network, vehicle-to-vehicle network, sensor network and so on.

MANET is characterized by having an open medium, dynamic topology, lacking of a centralized administration, and being bandwidth- and energy-constrained. These features make it difficult to deploy security mechanisms similar to that of in wired network. As a result, MANETs are more vulnerable than a conventional wired network and are susceptible to various kinds of attacks. In MANET, attack against its routing protocol (e.g. routing disruption and resource consumption) is particularly a serious problem.

At present, the Internet Engineering Task Force (IETF) MANET Working Group has standardized four routing protocols: AODV [1], DSR [2], OLSR [3], and TBRPF [4].

Most of the current research efforts (e.g. ARAN [5], Ariadne [6], SAODV [7], SEAD [8]–[14]) have focused on providing preventive schemes to secure the routing protocol in MANET. Most of these schemes rely on key management or encryption techniques to authenticate the routing message as well as prevent unauthorized nodes from joining the network. However, these approaches cannot prevent attacks launched by a compromised node who owns a legitimate key. To build a strong security mechanism, in-depth understanding on how malicious nodes can attack the MANET is indispensable.

In [15], Ning and Sun analyzed and evaluated several possible insider attacks against the AODV protocol including routing disruption and resource consumption attack. In [16], Hu et al. introduced a rushing attack which result in DoS attack on MANET when AODV protocol is used. The same authors also presented a wormhole attack as well as the countermeasure against the attack [17]. In [18], several passive attacks model against AODV protocol have been proposed. In [19], an approach to detect the attack which is launched by non-collaborating malicious node has been proposed. However, combined attack or colluding attack have not yet been well studied.

In this paper, we present a collusion attack model against the OLSR protocol. We show that it is possible for a pair of colluding attackers to prevent routes to a specific node from being established. In order to validate our analysis, we have implemented the attack in a network simulator and test the feasibility of the attack through simulations. After analyzed the attack in detail, we present a technique to detect the attack.

The rest of this paper is organized as follows. Section II describes an overview of the OLSR protocol. Section III presents a collusion attack model against the OLSR protocol. In section IV we show that the collusion attack can bring a devastating impact on the network performance through simulation-based experiment. Section V proposed a technique

1-4244-0357-X/06/$20.00 ©2006 IEEE

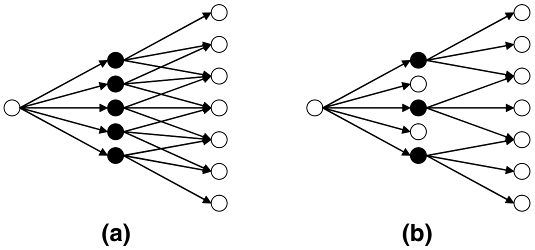

Fig. 1. The broadcast from the leftmost node is retransmitted: (a) by all its neighbors (b) by its MPRs only

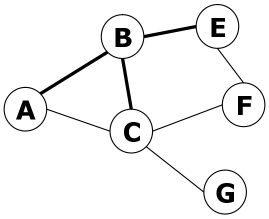

Fig. 2. Nodes A,C,E are neighbors of Node B

| originator | 1-hop neighbors |
|---|---|
| B | A,C,E |

Fig. 3. Example of Node B's HELLO message

to detect the collusion attack. Section VI describes our future works and concludes the paper.

## II. The Optimized Link State Routing (OLSR) Protocol

The Optimized Link State Routing (OLSR) protocol [3] is table driven, proactive routing protocol designed for mobile ad hoc networks. It employs periodic exchange of messages to maintain topology information of the network at each node. Based on topology information, each node is able to calculate the optimal route to a destination. In OLSR, routes are immediately available when needed.

The key concept of the protocol is the use of "multipoint relays" (MPR). Each node selects a set of its neighbor nodes as MPR. Only nodes, selected as such MPRs, are responsible for generating and forwarding topology information, intended for diffusion into the entire network. MPRs provide an efficient mechanism for flooding topology information by reducing the number of transmissions required. Fig. 1 illustrates a node broadcasts its messages throughout the network using standard flooding (Fig. 1 (a)) and MPR flooding (Fig. 1 (b)).

The core functionality of OLSR includes neighbor sensing, multipoint relays selection and topology diffusion. The followings describe each process.

### A. Neighbor Sensing

For neighbor sensing, the HELLO messages are broadcasted periodically. The HELLO messages are broadcasted only one hop away and are not forwarded further.

These messages are used to obtain the information about neighbors. A HELLO message performs the task of neighbor sensing and MPR selection process. A node's HELLO message contains its own address, a list of its 1-hop neighbors and a list of its MPR set. For example in Fig. 2, Node B's HELLO message contains its own address B and its 1-hop neighbors list A,C,E as shown in Fig. 3. Therefore, by exchanging HELLO messages, each node is able to obtain the information about its 1-hop and 2-hop neighbors and can find out which node has choosen it as a MPR.

### B. Multipoint Relays Selection

The idea of multipoint relays is to minimize the overhead of flooding messages in the network by reducing redundant retransmissions in the same region. Each node in the network selects a set of nodes in its 1-hop neighbors which may forward its messages. This set of selected neighbor nodes is called the "Multipoint Relay" (MPR) set of that node. When a node sends a routing message, only the nodes that are in its MPR set forward its message.

Each node constructs the MPR set which includes the minimum number of its 1-hop neighbors which it is possible to reach the node's all 2-hop neighbors.

Each node also maintains information about the set of neighbors that have selected it as a MPR. This set is called the "Multipoint Relay Selector set" (MPR selector set) of a node. A node obtains this information from periodic HELLO messages received from the neighbors. In OLSR, each node must forward the routing message, intended to be diffused in the whole network, coming from any of its MPR selectors.

### C. Topology Diffusion

In order to disseminate the topology information, the node that were selected as MPR must send the topology control (TC) message. The TC messages are the message that are intended to be flooded throughout the network and only MPR are allowed to forward TC messages. A node's TC message contains a list of its MPR selector set. For example, in Fig. 2, Node C and Node D's TC messages must contain the address of Node A who is one of their MPR selectors. Upon receiving TC messages of all MPR nodes in the network, each node learns all node's MPR set and hence obtains knowledge of the whole network topology. Based on these topology, the nodes are able to calculate routing table.

## III. The Model of Collusion Attack Against OLSR Protocol

In this section, we present a collusion attack in which two or more attackers collaborate each other to launch the attack in order to disrupt routing operation in OLSR MANET.

Fig. 4 shows a general image of the attack. Let Node T be the target to be attacked and let Node $A_1$ and $A_2$ be the colluding attackers. In the figure, $\{N_1, \ldots, N_i\}$ and $A_1$ is the subset of set $N$ which is the set of Node T's 1-hop neighbor nodes. $\{U_1, \ldots, U_i\}$ and $A_2$ is the subset of set $N_2$ which is the set of Node T's 2-hop neighbor nodes. $\{V_1, \ldots, V_i\}$ is the

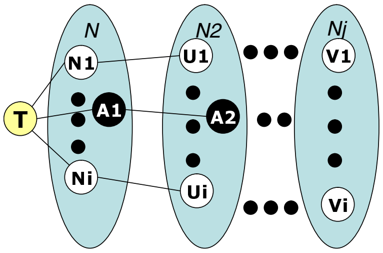

Fig. 4. A collusion attack model

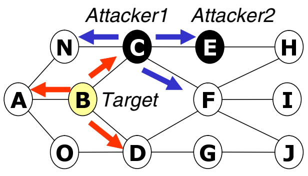

Fig. 5. The transmission of target's TC message under attack

| originator | 1-hop neighbors |
|---|---|
| C | E,F,G,N,O |

Fig. 6. Fake HELLO message generated by Node C

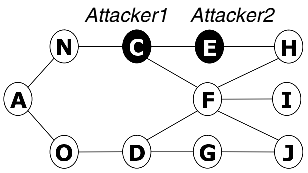

Fig. 7. Topology perceived by node H, I, J after the attack

TABLE I

SIMULATION PARAMETERS

| Simulator | NS-2 (ver.2.28) |
|---|---|
| Simulation time | 100 seconds |
| Transmission range | 250m |
| Link bandwidth | 2 Mbps |
| Traffic type | CBR |
| Data payload | 512 bytes |
| Packet rate | 4 pkt/s |
| Number of total nodes | 15 |
| Number of attackers | 4 |
| Number of connections | 1 |

subset of set $N_j$ which is the set of nodes whose distance to Node T is further than two hops.

In this attack, the first attacker $A_1$ advertises itself as having links to all target's 2-hops neighbors by sending a false HELLO message including the list of these neighbors' address, i.e, $\{U_1, \ldots, U_i\}$ and $A_1$. According to the protocol, $A_1$ will be chosen as the T's the only MPR. Therefore, $A_1$ will be the only node that can forward TC messages generated by Node T. $A_1$ then choose the second attacker $A_2$ as its the only MPR. By doing this, $A_2$ can perform the following misuses without being noticed by Node T.

(1) drop data packets or routing messages that pass through itself. For instance, $A_2$ can drop TC message which contains the address of Node T, i.e., TC message which is generated by $A_1$ and by T itself. This can cause link information of T to be unable to reach nodes whose distance is more than two hops, i.e, $\{V_1, \ldots, V_i\}$ and make these nodes unable to build a route to Node T.

(2) delete some of the contents in data packets or routing messages that pass through itself. For instance, $A_2$ can delete the address of T in TC message in order to make other nodes unable to build a route to Node T.

(3) modify data packets or message that pass through itself. For instance, $A_2$ changes the originator address of TC message generated by $A_1$ to make data packet destined to Node T being delivered to the wrong place.

(4) select $A_1$ as its only MPR in order to make TC message of Node T unable to reach other nodes.

The above mention attacks all can result in Denial of Service. These attacks are effective because the misbehavior is carried out outside the transmission range of the target which makes it difficult for the target to detect the anomaly behavior due to the attack.

Fig. 5 shows a concrete example of the attack. Firstly, Attacker1 (Node C) sends HELLO message including address list of target nodes (Node B) 's 2-hop neighbors, i.e, $\{E, F, G, N, O\}$ as shown in Fig. 6. According to the protocol, Attacker1 will become Node B's the only MPR. Secondly, Attacker1 choose Attacker2 (Node E) to be its the only MPR. Therefore, the TC message generated by target node will be forwarded by Attacker1 only (see the blue arrows). And this message must be forwarded by Attacker2 as well. However, instead of forwarding the message, Attacker2 drops this TC message. Furthermore, Attacker2 also drops TC message generated by Attacker1. Since the TC messages of Node B and TC messages of Attacker1 (who is Node B's the only MPR) does not reach other nodes (e.g., H,I,J), these nodes will not be able to build a route to Node B. The effect of this attack is illustrated in Fig. 7.

## IV. SIMULATION AND RESULTS

To validate our analysis, we have implemented the collusion attack in a simulator and performed series of simulation-based experiment to test its effectiveness. As a case study, we simulate the attack in which the first attacker advertise 2-hop neighbors of target node while the second attacker drops TC message. We run simulation on the network simulator NS-2 [20] using OLSR source code from [21]. The parameters used in our simulations are shown in Table I. In the simulation, the radio transmission range for each node is 250 meters and link bandwidth is set to 2 Mbps. The duration of simulation is 100 seconds. We use Constant Bit Rate (CBR) as the traffic source. The size of data payload is 512 bytes transmitted at the rate of 4 packets/s.

We simulated scenarios consisted of 15 wireless nodes including 2 colluding attackers and 1 target node on the 1000 meters by 1000 meters area. The target node moves according

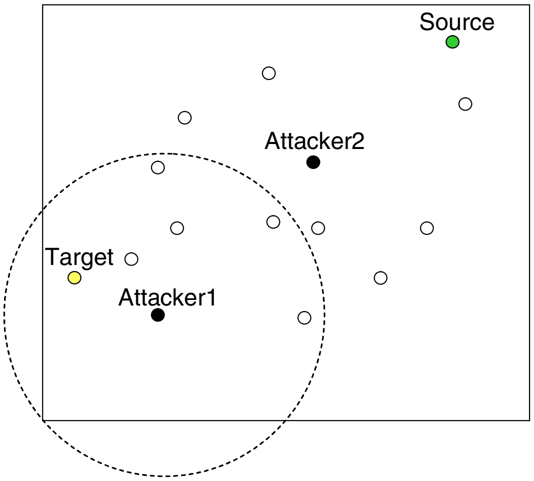

Fig. 8. Example of simulation topology

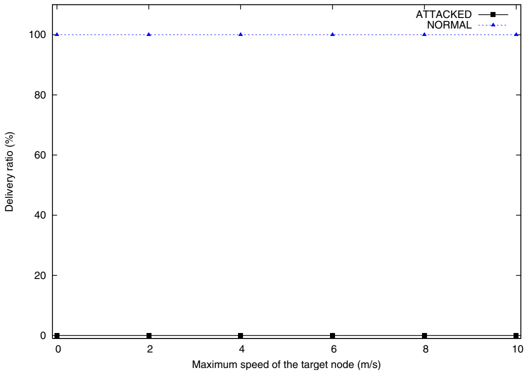

Fig. 9. Delivery ratio for varying maximum speed of a target node

to random waypoint model [22], i.e, after it arrives at a random location, it stays there for pause time seconds before moving to the next random destination and repeating the same process. Here we set the pause time to be 2 seconds. Attackers are placed such that their transmission range cover all area of target's movement. Fig. 8 shows an example of topology used in our simulations.

To test the feasibility of the attack, packet delivery ratio has been observed. Here, we define the delivery ratio as the ratio between number of data packets generated by the application layer CBR source and the number of packets received by the destination.

In the simulation, there are one CBR connection to a target node from a source node whose distance is further than two hops away from it. We vary the maximum speed of the target node from 0 m/s to 10 m/s in 2 m/s increments and observe the packet delivery ratio to a target node from a source node who is further than two hops away for each scenario.

The simulation results are shown in Fig. 9. As expected, when there is an attack, the delivery ratio drops to 0%, while in normal situation the target node can almost receive all generated data packets from the source node.

From these experiments, it is easy to see that attackers can effectively prevent a target node from receiving data packets from other nodes whose distance to a target node is more than two hops. This implies that, the attack can result in DoS attack to the target node.

## V. A Proposed Mechanism to Detect the Collusion Attack

In this section, we present a technique to detect the collusion attack in which the first attacker creates fake link to make the target's message route to itself while the second attacker misuses the message. Detecting whether or not the second attacker misuses the message is a non-trivial problem since the attack took place outside the transmission range of the target node. Therefore, it is important to detect the attack at early stage before the second attacker could launch the attack and magnify the damage. The following subsection describes the proposed method to detect the attack.

### A. *Detecting the Collusion Attack*

The collusion attack described in section III can be detected if each node is able to learn topology up to three hops.

Our approach requires each node to add its 2-hop neighbors list in its HELLO message in order to check whether link information advertised by its 1-hop neighbors is reliable or not. If any inconsistency has been found, a node conclude that there is an attack. In our solution, slight modification of an existing HELLO message has been made to include "2-hop neighbors" field which contains the address of a node's 2-hop neighbors. Therefore, by exchanging HELLO messages a node can learn topology up to three hops. Based on this information a node can find contradiction of link information obtained by each of its 1-hop neighbors.

Fig. 10 shows an example on how this mechanism works when Node C is the malicious node who aims to launch the attack against Node A. In the attack, in order to be Node A's the only MPR node C creates fake link with Node D who is A's 2-hop neighbors. In our solution, we require each node to send the list of its 1-hop neighbors as well as it's 2-hop neighbors. Thus, Node B's HELLO message contains node D who is its 1-hop neighbors and contains Nodes E, F and Z are B's 2-hop neighbors which have link with D as shown in Fig. 11. While Node C sends HELLO message as shown in Fig. 12. When Node A received HELLO message from both B and C, it judges the correctness of link information based on the received HELLO messages. From C's HELLO message, Node A learns that C is a neighbor of D. However, based on information from Node B, Node A learn that C is not a neighbor of D. In this way, Node A can detect the contradiction due to the attack.

### B. *Security Analysis*

Although by using the proposed mechanism, a node can detect the attack, it is still difficult to distinguish between the contradiction which is occured due to the attack or contradiction as a result of topology changes. Note that in the previous example, we cannot conclude that C is malicious,

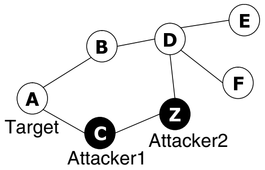

Fig. 10. Detecting the attack

| originator | 1-hop neighbors | 2-hop neighbors |
|---|---|---|
| B | D | E,F,Z |
| | A | C |

Fig. 11. HELLO message generated by Node B using the proposed mechanism

| originator | 1-hop neighbors | 2-hop neighbors |
|---|---|---|
| C | D | B,E,F,Z |
| | A | B |
| | Z | D |

Fig. 12. HELLO message generated by Node C using the proposed mechanism

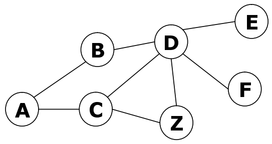

Fig. 13. Consideration on when Node C is a good node

since it is also possible that the contradiction that has been found is due to mobility. For example, consider the case shown in Fig. 13 where node C is a good node and is actually the neighbor of D. In this case, Node C's HELLO message will look like the one shown in Fig. 12. However, during the time Node B sends HELLO message the topology has been changed to the one shown in Fig. 10 due to nodes' mobility (e.g. Node C's mobility). In this case, Node B's HELLO message will look like the one shown in Fig. 11. In this situation, the same contradiction will be found as when there is an attack. Therefore, further investigation is required to distinguish between the case of the attack and the case of topology changes.

## VI. Conclusions

In this paper, we have presented a collusion attack in which the first attacker creates fake link to make packets route to itself while leting the second attacker to misuse the packet. The simualtion result showed that the attack can have a devastating impact on the OLSR MANET. After analyzed the attack, we have presented a simple mechanism to detect the attack by adding the address of 2-hop neighbors in HELLO message.

Our future work will be focused on implementing the proposed mechanism and evaluating its effectiveness as well as finding an efficient solution to avoid the attack.

## References

[1] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV) Routing," IETF RFC 3561, July 2003.

[2] D. B. Johnson, D. A. Maltz, and Y-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet Draft, draft-ietf-manet-dsr-09, April 2003.

[3] Th. Clausen et. al, "Optimized Link State Routing Protocol," IETF Internet Draft, draft-ietf-manet-olsr-11.txt, July 2003.

[4] R. Ogier, M. Lewis, and F. Templin, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," IETF Internet Draft, draft-ietf-manet-tbrpf-07.txt, March 2003.

[5] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Beldin-gRoyer, "A Secure Routing Protocol for Ad Hoc Networks," In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP), November 2002.

[6] Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," in Proceedings of the MobiCom 2002, Atlanta, Georgia, USA, September 23-28, 2002.

[7] M. G. Zapata, "Secure Ad hoc On-Demand Distance Vector Routing," ACM Mobile Computing and Communications Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002.

[8] Y-C. Hu, D. B. Johnson, and A. Perrig "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002.

[9] S. Capkun, L. Nuttyan, and J. Hubaux, "Self-organized public-key Management for mobile ad hoc networks," IEEE Transactions on mobile computing, Vol. 2, No. 1, January-March, 2003.

[10] L. Zhou, and Z. J. Haas, "Securing ad hoc networks," IEEE Networks Special Issue on Network Security November/December, 1999.

[11] C. Adjih, Th. Clausen, Ph. Jacquet, A. Laouiti, P. Muhlethaler, and D. Raffo, "Securing the OLSR protocol," In Proceedings of Med-Hoc-Net, Mahdia, Tunisia, June 25, 2003.

[12] D. Dhillon, T.S. Randhawa, M. Wang and L. Lamont, "Implementing a Fully Distributed Certificate Authority in an OLSR MANET," IEEE WCNC2004, Atlanta, Georgia USA, March 21-25, 2004.

[13] D. Raffo, C. Adjih, T. Clausen, and P. Muhlethaler, "An Advanced Signature System for OLSR," in Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN 04), Washington, DC, USA, October 25 2004.

[14] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security," 2nd OLSR Interop/ Workshop, Palaiseau, France, July 28-29, 2005.

[15] P. Ning, and K. Sun, "How to misuse AODV: A case study of insider attacks against mobile ad-hoc routing protocols," Tech. Rep. TR-2003-07, North Carolina State University, Department of Computer Science, February 2003.

[16] Y-C. Hu, A. Perrig, and D. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," ACM Workshop on Wireless Security (WiSe 2003) Westin Horton Plaza Hotel, San Diego, California, U.S.A, September 19, 2003.

[17] Y-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM), pp.1976-1986, 2003.

[18] X. Hong, J. Kong, and M. Gerla, "A New Set of Passive Routing Attacks in Mobile Ad Hoc Networks," in Proceedings of IEEE Military Communications Conference (MILCOM'03), Boston, MA, October 13-16, 2003.

[19] M. Wang, L. Lamont, P Mason, M. Gorlatova, "An Effective Intrusion Detection Approach for OLSR MANET Protocol", First Workshop on Secure Network Protocols (NPSec), Boston, Massachusetts, USA, November 6, 2005.

[20] The Vint Project, "The Network Simulator - ns-2," see http://www.isi.edu/nsnam/ns/index.html/.

[21] F. J. Ro, "UM-OLSR Documentation," University of Murcia, March 2005, see http://masimum.dif.um.es/um-olsr/html/.

[22] C. Bettstetter, G. Resta, and P. santi, "The Node Distribution of the Random Waypoint Mobility Model for Wireless Ad Hoc Networks," IEEE Transanction on Mobile Computing, Vol.2, No. 3, pp. 257-269, July/september, 2003.