Collusion Attack Resistance Through Forced MPR Switching in OLSR

Lalith Suresh P.[1], Rajbir Kaur[2], M.S.Gaur[3], V.Laxmi[4]
Department of Computer Engineering
Malaviya National Institute of Technology,
Jaipur, Rajasthan, India
Email: $\{$lalith[1]$|$rajbir[2]$|$gaurms[3]$|$vlaxmi[4]$\}$@mnit.ac.in

***Abstract*—Collusion Attack is an attack against Mobile Ad Hoc Networks and is based on Optimised Link State Routing (OLSR) Protocol. In this attack, two attacking nodes collude to prevent routes to a target node from being established in the network. Packet Delivery Ratio (PDR) of nodes 2-hops away from the victim drops to 0%. Multi Point Relay (MPR) selection process in OLSR is exploited to achieve route denial. In this paper, we propose a novel attack resistant method named Forced MPR Switching OLSR (FMS-OLSR), in which, whenever a node observes symptoms of the attack, it temporarily blacklists potential attackers. This forces recomputation of its MPR set, thus, avoiding the attack. Simulation results on *ns-3* show that FMS-OLSR is resistant to Collusion Attacks and incurs only a minimal penalty on network performance.**

I. Introduction

Mobile Ad Hoc Networks (MANETs) are wireless networks consisting of mobile nodes that communicate with each other without base stations. Since such network scenarios do not rely on centralised and organized connectivity, they generally find applications in places requiring rapid deployment by independent mobile users. MANETs are generally characterized as having dynamic topologies and are bandwidth and energy constrained.

MANETs are vulnerable to a wide array of network attacks. Collusion Attack [1] can easily be initiated in OLSR [2] based MANETs. The attack is launched by two colluding malicious nodes against a target node. Routes to target node cease to exist in the network. OLSR's MPR selection process is exploited to launch the attack. We propose a novel method FMS-OLSR which makes OLSR resistant to Collusion Attacks. FMS-OLSR works by ensuring that a node changes its MPR set proactively upon suspicion of the attack.

The rest of the paper is organized as follows : Section II describes the functioning of OLSR. Section III explains Collusion Attack. Section IV discusses related work. In Section V, we analyse convergence of collusion attack. Section VI presents proposed countermeasure, FMS-OLSR. Section VII explains possibility of network partitioning in our proposed system. We provide a formal analysis of the attack in VIII. Section IX provides simulation results and its analysis. Section X concludes our work.

II. Optimised Link State Routing Protocol

OLSR [2] is a proactive routing protocol for mobile ad hoc networks. Key optimisation in OLSR is the use of Multi Point Relay (MPR) nodes for controlled traffic flooding. Following subsections outline a brief description of the protocol.

A. Multi Point Relaying

In OLSR, only MPR nodes forward broadcast traffic. Each node calculates its MPR set by choosing a subset of its 1-hop neighbours, such that all its 2-hop neighbours can be reached through this MPR set. Nodes that select a particular node X as their MPR become MPR selectors for X. Smaller the MPR set, the lesser is amount of control message traffic generated.

B. Neighbour Discovery

HELLO messages are generated and transmitted at regular intervals to all 1-hop neighbours to achieve link sensing, neighbour sensing, two-hop neighbour-sensing and MPR selector sensing. Nodes transmit information about all known links and neighbours. The node's MPR set is also announced. Link information populates 1 and 2-hop neighbour repositories. An MPR set received via a HELLO message either updates or creates an entry in existing MPR selector set. MPR selector set of a node say A, consists of those nodes T, that have included A in their MPR set.

C. Link State Declaration

In OLSR, topology information is disseminated through the network using Topology Control (TC) messages. These messages are generated by MPR nodes at regular intervals (TC Interval) or whenever changes are detected in MPR selector set. Each MPR node advertises links between itself and nodes in its MPR selector set. Advertised Neighbour Sequence Number (ANSN) represents freshness of information contained in the message. MPR optimisation is used to flood TC messages in the entire network. TC messages are used to populate or update topology tuples in TC repository (topology set). After receiving a TC message, the topology set is updated as follows:

1) All tuples with $seqNo < ANSN$ are discarded. This is because this information is old. This is the **cancellation** of topology tuples.
2) For every advertised neighbour address received in the TC message: If it is a recent update to already existing information, the validity time of the existing information is increased.
   Else, a new tuple is created in the topology set.

978-1-4244-9228-2/10/$26.00 ©2010 IEEE

3) All tuples past their validity time are removed from the topology set. This is the **expiration** of topology tuples.

The local link information base (1 and 2-hop neighbour sets) and the topology set are used to calculate routes beyond 2-hop distance from any node [2]. The proposed heuristic for route calculation in [2] is a trivial shortest-path algorithm.

III. Collusion Attack Against OLSR

Topology information from TC messages is stored and processed by nodes to build routes to destinations that are more than 2-hops away from it [2]. In the collusion attack, the misbehaving nodes do not forward topology information related to the target node. This prevents routes to the target node from being established. As already stated, OLSR specifies that topology information (TC messages) is to be forwarded only by MPR nodes. Thus the **necessary condition for the attack** is that misbehaving nodes be MPR nodes. Consider the network in Figure 1. Let the misbehaving nodes (attackers) be *L* and *P* and let *T* be the target node. In this attack, the first attacker, node *L*, uses a HELLO message to announce symmetric 1-hop links to all the 2-hop neighbours of the target node *T*. As per the MPR Computation algorithm, *T* selects *L* as its MPR node. After being selected as an MPR node for *T*, the first attacker *L* chooses *P* as its own MPR node. This implies that all the TC messages generated by *L* are to be forwarded only by *P*. TC messages generated by *L* listing *T* as its MPR selector are dropped by *P*, the second attacker. No TC messages with information about the target node *T* are disseminated into the network. The result is that no node in the network will contain any topology tuple with information regarding *T*. Routes to *T* cannot be established by nodes more than 2-hops away from *T*. The effect of the attack is shown in Figure 2.

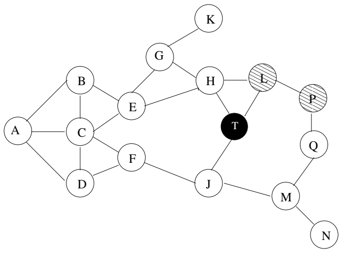

Fig. 1. A sample MANET. Node *T* is the target. Nodes *L* and *P* are colluding attackers

IV. Related Work

In [1], the authors propose to detect Collusion Attack by including a node's 2-hop neighbourhood information in HELLO messages. This allows a node to have knowledge of its 3-hop neighbours without the need of TC messages and to verify information sent by neighbours. Though the proposed method detects an attack, it cannot differentiate between mobility induced topology changes and the collusion attack. This results in a significant amount of false positives.

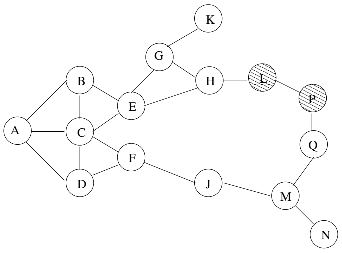

Fig. 2. Network Topology as seen by nodes beyond 2-hops distance from *T*, namely, *A, B, C, D, E, F, G, K, Q, N*

The authors in [3] propose incorporation of an information theoretic trust framework in OLSR to detect and act against Collusion Attack. Nodes cooperate to calculate trust values of other nodes, which leads to a blacklisting process after a certain threshold. This method involves maintaining extra data structures for storing the trust values at each node. Furthermore, the method requires cooperation of neighbouring nodes to arrive at correct results.

In [4], the authors address the problem of Collusion attack in OLSR using an acknowledgement (ACK) based mechanism to detect malicious nodes, so that they are excluded from the forwarding process. This scheme has a considerable overhead induced by the extra control messages.

In [5], the authors provide an analysis of the Node Isolation Attack, a version of Collusion Attack involving a single attacker. In the detection phase of the proposed countermeasure [5], the target observes its MPR node to check if it is generating TC messages. This approach fails against the Collusion Attack because it is the second attacker that drops packets and this attacker may be outside the target's range.

In contrast to the above mentioned methods, our proposed method, FMS-OLSR, does not involve any new kind of packet format or processing. Furthermore, the memory and CPU requirements for FMS-OLSR are expected to remain minimal, making it well suited for MANETs.

V. Collusion Attack Convergence

Initially we assume that all nodes are honest. MPR nodes of the target (*T* in Figure 1) generate TC messages advertising *T* as their neighbour. We refer to this set of MPR nodes of *T* as $MPRSet_{before}$. Therefore, nodes at a distance of 3-hops from *T* will have routes to it in their routing tables. When the attack is initiated, the target *T* receives a fake HELLO message from the first attacker *L* and *T* recomputes its MPR set. The new MPR Set of *T*, referred to as $MPRSet_{after}$, will have only one element *L*. After a duration equal to the HELLO interval, *T* generates a HELLO message indicating *L* as its only MPR. All nodes in $MPRSet_{before}$ remove *T* from their MPR Selector set. The subsequent TC messages generated by the nodes in $MPRSet_{before}$ will not contain any connectivity information regarding *T*. All TC messages generated by *L* are dropped by colluding attacker *P*. Hence, no TC messages from *L* disseminate into the network. The result is that topology tuples with information about *T* will expire eventually and will be removed from the topology set. The collusion attack converges when all nodes at 3-hops distance from the target no longer have routes to it. We discuss two possible delays in the convergence of the collusion attack.

1) *Short Convergence Delay*: Let L not be in $MPRSet_{before}$. This means that no topology tuples before the attack would have been generated from L's TC messages. After the attack, if nodes in $MPRSet_{before}$ have non-empty MPR Selector Sets, they will further generate TC messages. These TC messages will not announce any link to *T* and will cancel all topology tuples with information about *T*(**cancellation** of topology tuples). The upper time bound for this to happen is the time between two TC messages. This time is equal to the TC-interval.
2) *Long Convergence Delay*: If the set of nodes *X* in $MPRSet_{before}$ have empty MPR Selector sets, they will not generate any more TC messages. Hence, topology tuples generated before the attack due to TC messages from *X* will expire. The attack will succeed once all these topology tuples expire (**expiration** of topology tuples). The time required for this is the Topology Holding Time which is, typically thrice the TC-Interval.

VI. Forced MPR Switching OLSR (FMS-OLSR)

The key to executing a Collusion Attack is to force the target node to choose one of the attackers as its only MPR node. In FMS-OLSR, we work around this by always ensuring that a node has more than one MPR node in its MPR set. While this could lead to non-optimal MPR sets, we show in Section IX that this does not have a significant impact on the network's performance. In FMS-OLSR, as soon as a node *X* generates a HELLO message, it checks the number of nodes in its MPR set. If the number of nodes in the MPR set is 1, it checks its 1-hop neighbour set *N1*. If *X* has more than one neighbour, it adds the lone MPR to an $AvoidanceSet$ after waiting for a duration $AvoidanceDelay(AvDelay)$. All entries in the $AvoidanceSet$ of *X* are not included in its MPR computation process. These entries are removed from the $AvoidanceSet$ after a duration $AvoidanceHold(AvHold)$. When *X* generates another HELLO message (which indicates the new MPR set), the new MPR neighbours will add *X* to their MPR Selector sets again. The next set of TC messages that are generated by these new MPR nodes will announce topology information regarding *X*. This nullifies the attack. By carefully choosing values for $AvDelay$ and $AvHold$, we can cancel the attack before it converges.

According to our proposal, as soon as target node *T* generates a HELLO message, it checks the size of its MPR set. During attack, *T*'s MPR set will contain a lone MPR node, namely, attacker *L*, which colludes with attacker *P* to prevent information regarding *T* to be disseminated into the network. Finding a lone entry in it's MPR set, *T* will check its 1-hop neighbour set. Since *T* has more than one 1-hop neighbours, it adds L to its $AvoidanceSet$ after a duration $AvDelay$. So, L will not be included in MPR recomputation process. Now, T generates another HELLO messages announcing its new MPR set. Nodes in MPR set will include *T* in their respective MPR Selector sets. The next set of TC messages generated by new MPR nodes will announce topology information regarding *T*. Hence topology information of *T* will again be disseminated into the network. Thus the affect of the attack will be nullified.

Short Convergence Delay = TC-Interval
*Long Convergence Delay = 3 * TC-Interval*

After the attack is launched, new MPR set is calculated and announced in next HELLO message. If this HELLO message is processed by new MPR nodes before they generate next set of TC messages, attack will never take effect. To this end, if $AvDelay$ is kept below TC-Interval, attack can be cancelled within the next one or two set of TC messages. The following Equations should be satisfied to ensure that the attack is cancelled before it converges:

$$\textit{AvDelay + HELLO-Interval} < \textit{Convergence Time} \;....\; (1)$$
$$\textit{AvDelay + AvHold + HELLO Interval} > \textit{Convergence Time} \;....\; (2)$$

Equation (1) implies that lone MPR should be blacklisted and the target should announce new MPR set before attack can converge. Equation (2) implies that a node should never be removed from the blacklist before the attack can converge (lest it cancels the recovery process). HELLO Interval is included in the equation so that new MPR set can be announced by the target to neighbours before generation of TC messages. The neighbours can then recompute their MPR Selector sets and generate TC Messages to cancel the attack. Note that this model will also work against a chain of colluding attackers of any length (including Node Isolation Attack [5]).

VII. Possibility of Network Partitioning in FMS-OLSR

As long as a node *A* is in *T*'s Avoidance-Set, *A* will never generate TC message stating *T* as MPR Selector. Route to *T* can only be established by nodes that are more than 2-hops away from *T*, if and only if *T* has another MPR node. We now examine two cases where a node has only two neighbours, and how OLSR and FMS-OLSR handle each case.

Case I: In Figure 3, node *T* is the only link between two halves or portions of the network. *T* has only two 1-hop neighbours *A* and *E*. It is impossible for node *T* to have only one MPR. If *T* has only one MPR node after the MPR computation process, it indicates that the lone MPR has sent a spoofed HELLO message (Collusion Attack initiation). A node

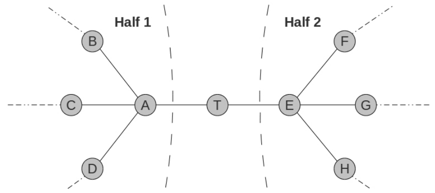

Fig. 3. Case I: If link *A-T* or *T-E* is not announced through TC messages, the network becomes partitioned

from Half 1 cannot have a 1-hop link to a node in Half 2 and vice versa. In Figure 3, if *T*'s MPR set is $\{A\}$, it implies that *A* has sent a fake HELLO message. Let *B* be second attacker.

1) OLSR: Node *A* being *T*'s only MPR is the only node allowed to generate TC messages for *T*. These TC messages are dropped by *A*'s only MPR *B*. Since no TC messages being generated in the network announce links *T-A* or *T-E*, communication between legitimate nodes from either half of the network becomes impossible.
2) FMS-OLSR: As soon as node *T* observes that it has only one MPR node, it waits for the $AvDelay$ duration and blacklists node *A*. It then picks *E* as its MPR. Link *T-E* is announced but node in Half 1 may not communicate to node in Half 2 as all communication through the link is at the mercy of malicious node *A*. This is unavoidable under any circumstance.

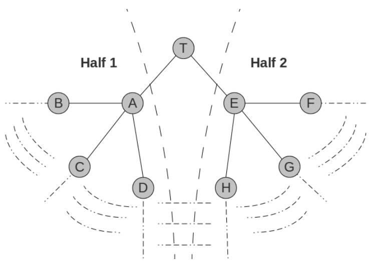

Fig. 4. Case II: If link *A-T* or *T-E* is not announced through TC messages, the network does not become partitioned and node *T* can still communicate to rest of the network

Case II: In Figure 4, there are links between two halves of the network. *T-A* and *T-E* are not the only links that have to fail for the network to partition. *A* and *B* are attackers.

1) OLSR: *A* generates TC messages with information about *T*. These TC messages are dropped by *B*. Since none of these TC messages reach rest of the network, routes to *T* cease to exist after convergence period.
2) FMS-OLSR: Once *A* executes the attack and becomes *T*'s only MPR, *T* proceeds to blacklist *A* and avoids including it in MPR Computation process for $AvHold$ duration. *E* becomes *T*'s only MPR. *E* then generates TC messages. Since network is not partitioned, communication to T from Half 1 is still possible through remaining links between two halves.

If target node has only one neighbour, as per FMS-OLSR no blacklisting takes place. This is acceptable as the only link target node has with the network is through its only neighbour and MPR. If this neighbour is a legitimate node, target can communicate with rest of the network. If all neighbours of a node are malicious, target is at mercy of these malicious nodes. There is no known solution for this situation.

VIII. FMS-OLSR Analysis

We now provide an analysis of FMS-OLSR with respect to a generalised version of the Collusion Attack extended upto any number of colluding attackers. We define the following:

- N_{leg}: Set of legitimate nodes.
- N_{att}: Set of attackers (colluding nodes)
- Collusion Chain: An ordered set of attackers $\{A_1, A_2, A_3$ ... $A_c\}$, where *c* is the length of collusion chain, A_1, head, sends spoofed HELLO message to initiate the attack, A_c, tail of the chain, drops the packets of the victim and all attackers $A_1, A_2 ... A_{c-1}$.
- A_k: k^{th} attacker in the chain.
- $A \rightarrow B$: *B* is in *A*'s MPR set.
- $A \rightsquigarrow B$: There exists a set of nodes $\{X_1,\ X_2\ ...\ X_k\}$ $\notin N_{att}$ such that $A \rightarrow X_1 \rightarrow X_2 ... \rightarrow X_k \rightarrow B$ is true. For a node *X* to have an attack free route to a node *A*, $A \rightsquigarrow X$ should be true. Only then TC messages with connectivity information about *A* will reach *X*.

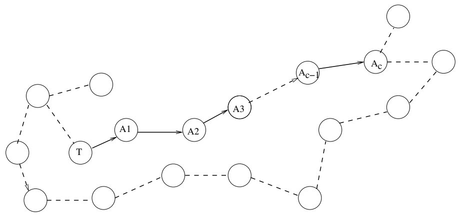

Fig. 5. Collusion attack chain A_1 to A_c targeting *T*

Consider the topology in figure 5. When collusion attack is executed, the target node *T* has only one MPR node A_1, indicated by outgoing edge from *T* in the graph. In above scenario, assume that there is atleast one node *B* which has attack free routes to *T*. This means that $T \rightsquigarrow B$ is true. Necessary condition for collusion attack to take place is that the head of collusion chain must be the only MPR node of the target. The only outbound edge from the target *T* is to a node $\in N_{att}$. Thus, in the above mentioned sequence, $A_1 == X_1 \in N_{att}$. Thus $T \rightsquigarrow B$ cannot be true. This implies that routes cannot be formed to *T* in such a scenario.

With FMS-OLSR, the target *T* detects the symptoms of the attack and proceeds to blacklist A_1 temporarily (provided that for *T*, $|N1| > 1$). *T* change its MPR set to include a legitimate node (thus eliminating the necessary condition for the attack). All nodes $X \in N_{leg}$ for which $T \rightsquigarrow X$ is true will have routes to *T*. This allows *T* to work around collusion attack.

IX. Simulation Results

We verified FMS-OLSR using *ns-3* [6]. OLSR module of *ns-3* is modified to implement FMS-OLSR and to allow execution of Collusion Attack. There is one target and a pair of colluding attackers. A single source sends UDP packets to the target from 30th second onwards. Collusion Attack is launched at 36th second. All nodes move with same speed which is varied between 0 and 10 m/s. Default values of HELLO and TC Interval as per [2] are used. For a TC interval of 5 seconds, expected convergence time for Collusion Attack is either 5 seconds ($ShortConvergenceDelay$) or 15 seconds ($LongConvergenceDelay$). $AvHold$ is chosen to be 20 seconds to keep Equation (2) in Section VI always true.

TABLE I
SIMULATION PARAMETERS

Number of Nodes	36
Area	2400 x 2400 square meters
Signal Range of each node	500 meters
Mobility Model	Random Direction Waypoint Model
Number of packets sent from source to destination	1000
Simulation Time	150 seconds
HELLO Interval	2 seconds
TC Interval	5 seconds

Figure 6 shows the variation in PDR versus speed of the nodes for different values of $AvDelay$. PDR is better for lower values of $AvDelay$, with the best performance being observed for a value of 2 seconds. This is because sooner a node blacklists a lone MPR, more are the chances that attack will be nullified before it converges.

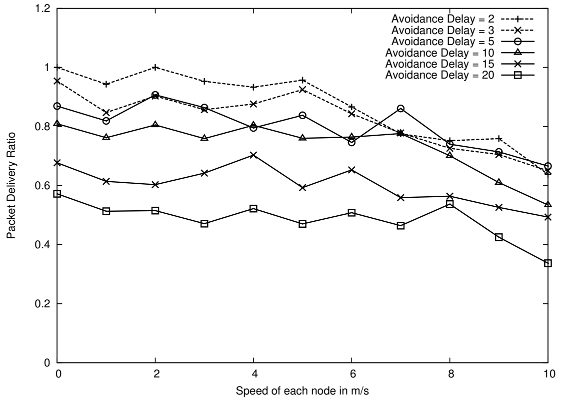

Fig. 6. PDR versus Speed for different values of Avoidance Delay, when the target is under a collusion attack

Figure 7 compares OLSR and FMS-OLSR. When OLSR is under attack, PDR drops to very low values. The only packets received by the node is during convergence of attack. No packets are received after convergence. PDR curve with FMS-OLSR (under attack and otherwise) is comparable to that of OLSR without attack. FMS-OLSR is highly resistant to the Collusion Attack.

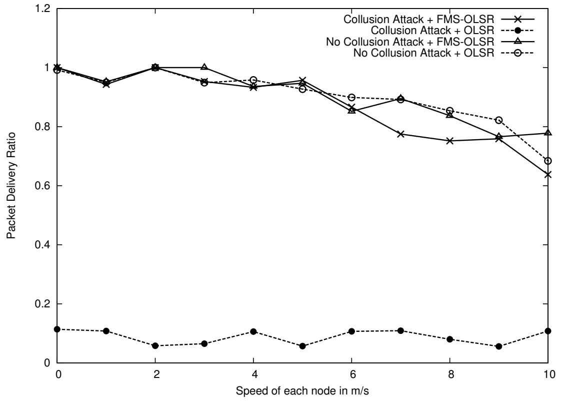

Fig. 7. PDR versus Speed of each node under different scenarios

In Figure 8, extra control packets generated in FMS-OLSR (with and without attack) and OLSR (without attack) are compared. Extra control packets are generated in FMS-OLSR due to the computation of non-optimal MPR sets. We observe from Figure 8 that the number of control packets generated in FMS-OLSR is comparable to OLSR without attack. FMS-OLSR is well suited for MANETs wherein mobility is an important characteristic of the nodes.

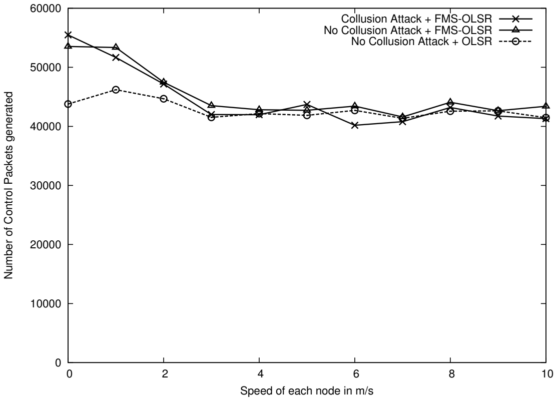

Fig. 8. Control Packet Overhead versus speed for different scenarios

X. CONCLUSION

This paper proposes a novel Collusion Attack Resistant variant of OLSR named FMS-OLSR. Simulation results demonstrate that proposed method is effective in thwarting Collusion Attack. Results also prove that FMS-OLSR does not affect network performance significantly while providing collusion attack resistance. The observed overhead is comparable to that of OLSR without attack. Being an intuitively simple method without any significant processing overhead, FMS-OLSR is well suited for implementation in MANETs which are constrained by memory and energy resources.

REFERENCES

[1] A. Jamalipour B. Kannhavong, H. Nakayama. A collusion attack against OLSR-based mobile ad hoc networks. In *Global Telecommunications Conference. IEEE*, pages 1 – 5, November 2006.

[2] P. Jacquet, P. Mhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks, 2001.

[3] K.B. Madasu, A. Franklin, and C.S.Ram Murthy. On the prevention of collusion attack in OLSR-based mobile ad hoc networks. In *IEEE International Conference on Networks*, pages 1–6, December 2008.

[4] S. Djahel, F. Nat-Abdesselam, Z. Zhang, and A. Khokhar. Defending against packet dropping attack in vehicular ad hoc networks. *Security and Communication Networks*, 1(3):245–258, 2008.

[5] K. Bounpadith, N. Hidehisa, K. Nei, J. Abbas, and N. Yoshiaki. A study of a routing attack in olsr-based mobile ad hoc networks. *Int. J. Commun. Syst.*, 20(11):1245–1261, 2007.

[6] Network simulator 3. http://www.nsnam.org.