**Mitigating Denial of Service Attacks in OLSR Protocol Using Fictitious Nodes**

**ABSTRACT:**

With the main focus of research in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the resulting protocols tend to be vulnerable to various attacks. Over the years, emphasis has also been placed on improving the security of these networks. Different solutions have been proposed for different types of attacks, however, these solutions often compromise routing efficiency or network overload. One major DOS attack against the Optimized Link State Routing protocol (OLSR) known as the node isolation attack occurs when topological knowledge of the network is exploited by an attacker who is able to isolate the victim from the rest of the network and subsequently deny communication services to the victim. In this paper, we suggest a novel solution to defend the OLSR protocol from node isolation attack by employing the same tactics used by the attack itself. Through extensive experimentation, we demonstrate that 1) the proposed protection prevents more than 95 percent of attacks, and 2) the overhead required drastically decreases as the network size increases until it is non-discernable. Last, we suggest that this type of solution can be extended to other similar DOS attacks on OLSR.

**EXISTING SYSTEM:**

* In the existing system, every node inspect its MPRs’ TC messages to see whether it has been included. This is possible due to the nature of the broadcast channel in wireless networks and also because MPR selection rules exclusively allow for the designation of MPRs within broadcast distance only.
* The existing system can conclude whether x is malicious by looking for its own address in x’s TC message; its lack thereof can only be due to malicious intent. This solution is elegant, but it has a number of drawbacks. First, this scheme is only effective against a single attacker, but, as the authors note, it fails in situations involving two consecutive colluding attackers. By having the first attacker orchestrates the attack yet advertise the correct TC, the victim cannot tell that it is under attack.
* The second colluding attacker, designated as the first’s sole MPR, removes the victim from the advertised TC prior to propagation, isolating it from the network.

**PROPOSED SYSTEM:**

* In the existing system, the system reviews a specific DOS attack called node isolation attack and proposes a new mitigation method. Our solution called Denial Contradictions with Fictitious Node Mechanism (DCFM) relies on the internal knowledge acquired by each node during routine routing, and augmentation of virtual (fictitious) nodes.
* Moreover, DCFM utilizes the same techniques used by the attack in order to prevent it. The overhead of the additional virtual nodes diminishes as network size increases, which is consistent with [4]’s general claim that OLSR functions best on large networks.

**SYSTEM ARCHITECTURE:**

**SYSTEM SPECIFICATION**

**Hardware Requirements:**

* System : Pentium IV 3.5 GHz.
* Hard Disk : 40 GB.
* Monitor : 14’ Colour Monitor.
* Mouse : Optical Mouse.
* Ram : 1 GB.

**Software Requirements:**

* Operating system : Windows XP or Windows 7, Windows 8.
* Coding Language : Java – AWT,Swings,Networking
* Data Base : My Sql / MS Access.
* Documentation : MS Office
* IDE : Eclipse Galileo
* Development Kit : JDK 1.6