INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 3 ISSUE 2 (2017) PAGES 2004 – 2012
RECEIVED: 15-03-2017. PUBLISHED: 04-04-2017.

April 04, 2017

DETECTION AND PREVENTION OF DDoS ATTACK USING MODERN CRACKING ALGORITHM

[1]S.G.Suganya, [2]D.Prasanna,
[1]PG Scholar, Dept Of CSE, Mahendra Engineering College,
[2]Asst Prof, Dept Of CSE, Mahendra Engineering College.

ABSTRACT

Among the most important center of attention of examine in routing protocols for Mobile Ad-Hoc Networks (MANET) geared towards routing efficiency, the consequential protocols have a propensity to be defenseless to various attacks. In excess of the existence, prominence has as well been positioned on improving the protection of these networks. Different solutions have been planned on behalf of dissimilar types of attacks; nevertheless, these solutions often compromise direction-finding efficiency or network overload. One major DOS attack touching the Optimized Link State Routing protocol (OLSR) known as the node separation assail occurs while topological knowledge of the network is demoralized by an attacker who is proficient to isolate the wounded inauguration the relief of the network and consequently refuse communication services to the victim. In this project, we suggest a novel solution to defend the OLSR protocol beginning node isolation attack by employing the equivalent procedure worn by the assail itself. All the way through extensive testing we make obvious that 1) the proposed security prevents supplementary than 95% of attacks, and 2) the overhead required considerably decreases as the network size increases in anticipation of it is non-discernable. Last but not least, these projects suggest that this type of resolution can be extended to other similar DOS attacks on OLSR.

Keywords: Optimized Link State Routing protocol (OLSR), Mobile Ad-Hoc Networks (MANET), Multi Point Relays (MPRs), Multiple Interface Declaration (MID), Route Request (RReq)

1. INTRODUCTION

Ad-hoc networks are not restricted to any special hardware. But today such networks are most likely to consist of nodes utilizing so-called WLAN interfaces.Collecting information from each protocol and an evaluating this information. Choosing the best values for protocol parameters in order to improve the performance. Sending and receiving packets of other nodes running a different protocol. Creating an Ad Hoc Framework architecture based on multiprotocol nodes

- Nodes run different routing protocols
- Protocols collaborate during the lifetime of the Ad Hoc network

Studying pro and re-active protocols working together. Exploring new algorithms for Ad Hoc networks

- Proactive protocol

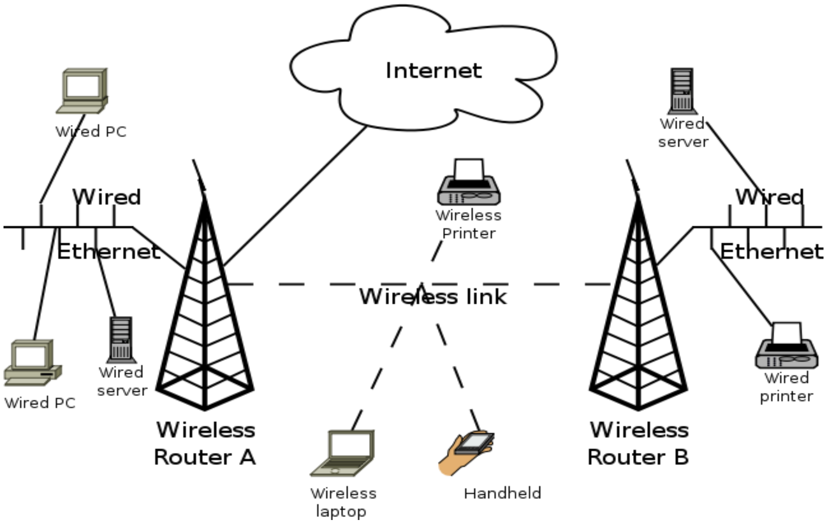

Figure.1. Wireless Networks

  - Link state based (routes are known beforehand)
- Exchange topology information with other nodes of the network regularly
- Based on Multi Point Relays (MPRs)
  - MPRs minimize flooding
  - Selected nodes which forward broadcast messages during the flooding process

AODV possibly will not find OLSR nodes but OLSR nodes could find AODV nodes. Very good behaviour (similar to previous case). Ordinary modules worked very well and central node managed perfectly both protocols.

The functioning of OLSR into two groups

- Core Functioning- always required for the protocol to operate.
- Auxiliary Functioning- provides additional functionality, which may be applicable in specific scenarios.

In a table-driven protocol such as OLSR, basically ever thing is related to tables (repositories, databases). These tables need to be maintained both upon receiving information and regarding the time received information is to be considered valid (timeout). All route calculation and most packet generation is based on these tables.

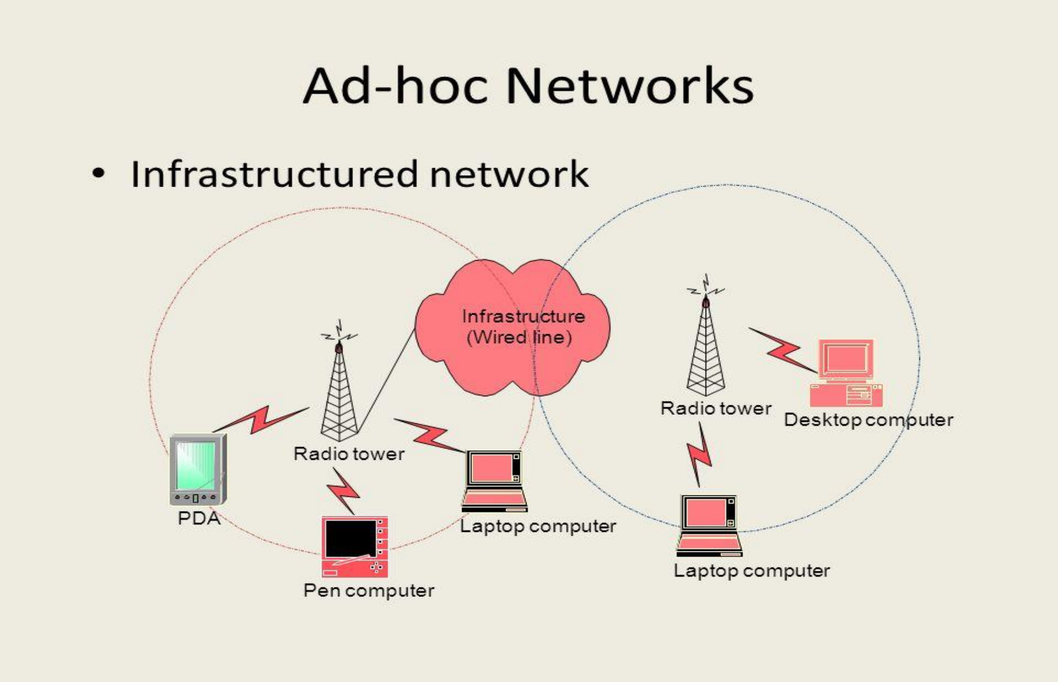

Figure.2. A traditional base station scheme compared to an ah-hoc multi-hop network.

2. RELATED WORKS

OLSR defines a default forwarding algorithm ensuring that all known and unknown message-types are forwarded according to the MPR optimization. To avoid synchronization when forwarding a jitter is used. This means that a message is to be cached in the node for a random time interval before forwarding it. Due to this messages are often “piggybacked” – one OLSR packet contains several OLSR messages. In OLSR a nodes IP address is used as an identification. So all nodes must set one main address. If only using one interface this interfaces IP address (IP header source) is used. If running OLSR on multiple interfaces one address must be chosen. And used as originator in all OLSR packets. To announce the usage of several interfaces (IPs) Multiple Interface Declaration messages are flooded. The Dynamic Source Routing protocol (DSR) is a straightforward and efficient routing protocol calculated distinctively for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. The overhead of flooding link state information is reduced by requiring fewer nodes to forward the information. A road cast from node X is only forwarded by its multipoint relays Multipoint relays of node X are its neighbors such that each two-hop neighbor of X is a one-hop neighbor of at least one multipoint relay of X. Each node transmits its neighbor list in periodic beacons, so that all nodes can know their 2-hop neighbors, in order to choose the multipoint relays

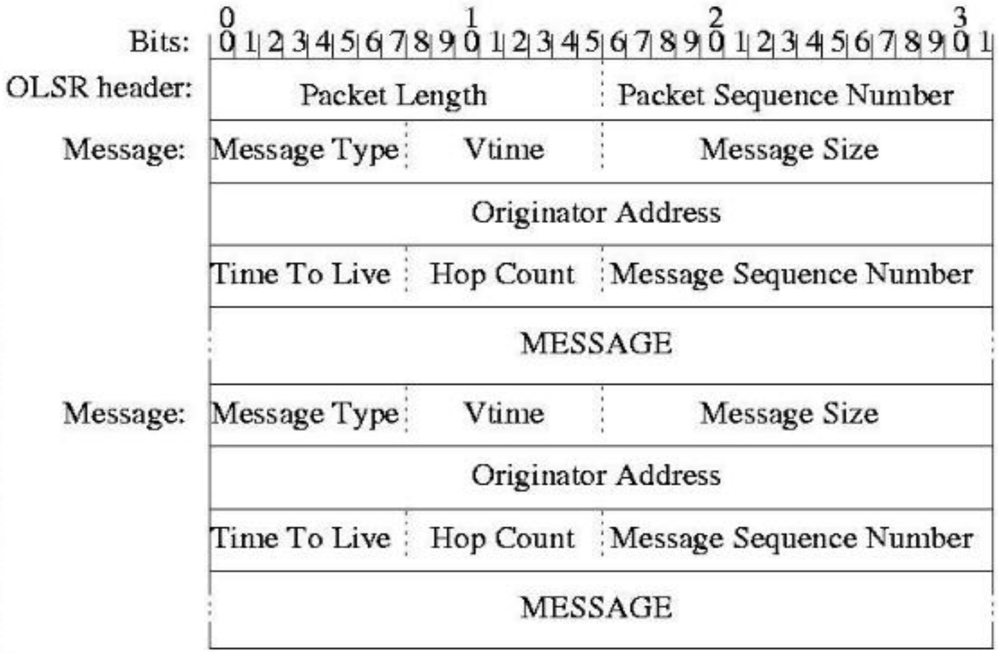

Figure.3. OLSR Packet Format

3. EXISTING SYSTEM

Assess control chart, a tool used in statistical process control (SPC) used for detecting DOS which produces low detection and high false alarm rates. In order to overpower those demerits they implemented adaptive intrusion detection and prevention (AIDP) mechanism, Initially uses chi-square test as an Anomaly based intrusion detection mechanism to examine the overall behavior of the network and then uses control chart for identifying intruder nodes. Finally isolates the intruder nodes.

Merits

- AIDP exhibits a high success rate and very low false alarm rate with an affordable processing overhead on the network over a range of scenarios tested.

Demerits

- Misused based intrusion detection (MBID) is not used, AIDP is more prone to generate false positives than MBID and also a reasonable processing overhead on the network.

4. PROPOSED SYSTEM

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 general claim that OLSR functions best on large networks. DCFM is unique in that all the information used to protect the MANET stems from the victim’s internal knowledge, without the need to rely on a trusted third party. In addition, the same technique used for the attack is exploited in order to provide protection. By learning local topology and advertising fictitious nodes, a node is able to deduce suspect nodes and refrain from nominating them as a sole MPR, thus, sidestepping the essential element of the attack

Rewards

- DCFM successfully prevents the attack, specifically in the realistic scenario in which all nodes in the network are mobile
- it was discovered that as node population increases in density and size, the closer DCFM overhead is to OLSR
- OLSR functions best in dense large networks, DCFM can function without real additional cost

5. PROCESS

A table-driven, pro-active protocol Optimized by Multi Point Relay flooding and messaging. Generates a constant overhead of control traffic No route lookup delay. OLSR uses two kinds of the control messages: Hello and Topology Control (TC). Hello messages are used for finding the information about the link status and the host’s neighbours. With the Hello message the Multipoint Relay (MPR) Selector set is constructed which describes which neighbours has chosen this host to act as MPR and from this information the host can calculate its own set of the MPRs. The Hello messages are sent only one hop away but the TC messages are broadcasted throughout the entire network. In Mobile Ad Hoc Networks (MANETs), mobile nodes use wireless devices to create spontaneously a larger network, larger than the one hop radio range, in which communication with each other is made possible by the means of routing. The goal of this document is the study of security issue related to integrity of an ad hoc network. We only consider ad hoc networks using the OLSR routing protocol. In a previous research report we have carried out a theoretical analysis of this issue. In this document we aim at precising a detailed security using the OLSR routing protocol.

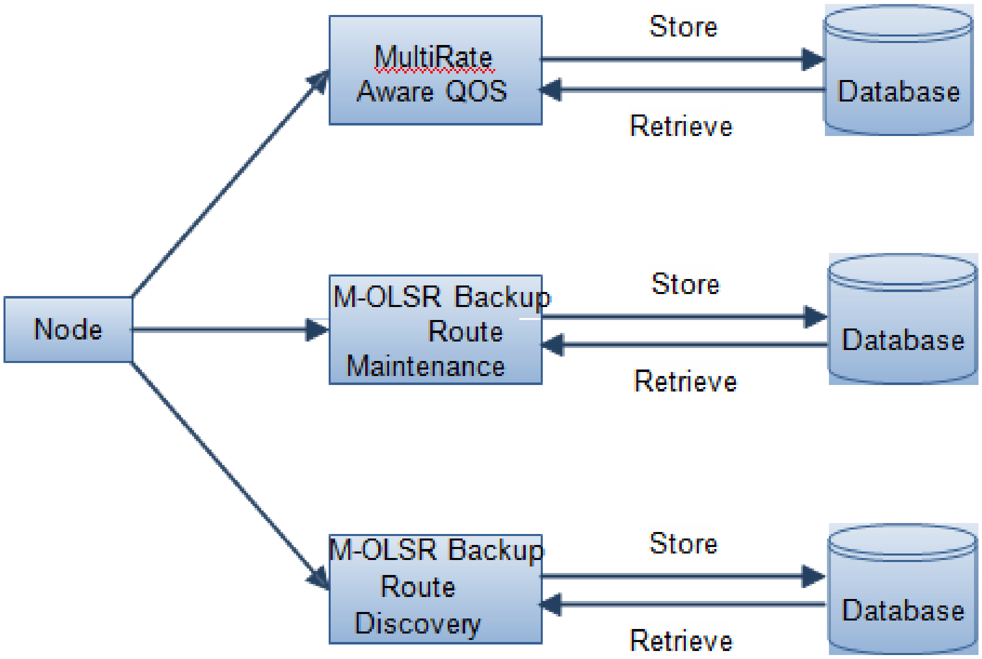

Figure.4. System Architecture Block Diagram

Modified DSR protocol: Detection and Removal of selective black hole attack in MANET

- The source node forwards the block of packet to the destination nodes once the packet reach the destination the probability of data reached is calculated if its value is greater than threshold value of packet loss then it initiates the gray hole detection procedure.
- The destination node begins the detection of the presence of malicious attacks in the source route using query request and mark it as suspicious nodes.
- The IDS nodes that are adjacent to the suspected nodes turn into promiscuous mode and hear whether the data packets are forwarded or dropped by the suspected nodes.

6. SYSTEM MODEL

- Node Deployment
- M-OLSR Route Backup
- Backup Route Maintenance
- Multi rate Aware QoS

Node Deployment

- In this module, we construct a topology structure. Here we use mesh topology because of its unstructured nature. Topology is constructed by getting the names of the nodes and the connections among the nodes as input from the user.

- While getting each of the nodes, their associated port and ip address is also obtained. For successive nodes, the node to which it should be connected is also accepted from the user. While adding nodes, comparison will be done so that there would be no node duplication. Then we identify the source and the destinations.

There are two types of nodes

- Device Node
- Execution Environment Node

M-OLSR Route Backup

- In the newly proposed protocol, once a session being admitted by M-OLSR has found a suitable route and its CS neighbors have been tested during the SREQ/SREP exchange, a backup route for the session must be found.
- There are two possible cases. Either more than one route to the destination of the session is already known, or a backup route must be discovered.
- If a new backup route must be discovered, the search packet, referred to as RReq backup carries a copy of the session's primary route.
- To avoid fully flooding the network with the RReq-backup, once the RReq backup has traveled at least half of the length of the primary route, the dis jointness condition is enforced and the packet is dropped if the partially discovered route does not comply

Backup Route Maintenance

- Capacity query messages send to retest backup routes to ensure that they still have sufficient capacity to support their corresponding data session. This incurs extra overhead. By contrast, M-OLSR backup avoids this overhead in the following manner:
- The lists of nodes comprising a session's primary and backup routes are delivered to the backup route's nodes via the SREP backup packet.
- Each backup route node continually monitors its CS neighborhood capacity using the aforementioned lower NCS monitoring threshold. Once per second, in the same manner as for the original SREQ backup driven route test, each node tests if its residual capacity could still support the session, in case it was rerouted to the backup route.
- If not, a reject message is sent to the source node, containing the rejected route. This message is only forwarded by any node that has knowledge of the session, provided furthermore that the rejected backup route matches the record of the backup route stored for the session.

- If the source node still has the rejected route stored as a backup route, it erases the corresponding record from the session state information table (but not from the route cache, as it is still valid routing information), marks the route as "unusable" (by that session) for a timeout period, and attempts to find a new backup route.

Multi rate Aware QoS

- The first stage consists of capacity-constrained route discovery, wherein each node forwards the flooded route request (RReq) or the route reply (RRep) if and only if it has sufficient capacity to support the session.
- In our implementation, each node stores the rate that was last used for transmission to each of its neighbors with which it has communicated, as well as the numbers of contiguous missed or received ACKs.
- Instead, the rate in use by each packet is recorded, and the average rate is calculated by a sliding window. This average rate is rounded off to the nearest supported rate, which is reported to the routing protocol when it queries that particular link rate.

M-OLSR Algorithm for MPR (Multi Point Relay) Selection

- Start with an empty multipoint relay set.
- Firstly, select those 1-hop neighbor nodes in N1 as multipoint relay nodes which provide the only path to reach some 2-hop neighbor nodes in N2 and add these 1- hop neighbor nodes to the multipoint relay set MPR(x).
- While there exist nodes in N2 which are not yet covered by at least one node in the MPR(x) set:
  - Add nodes in Nl to MPR(x) which offer the best feasible 1-hop path in terms of maximum value of f (p).
  - Mark the 2-hop neighbor as covered.
- Repeat the above process until all the 2-hop nodes are reachable via at least one of its MPR nodes.

CONCLUSION

This Project describes the Optimized Link State Routing (OLSR) protocol for mobile ad hoc networks. The protocol is an optimization of the classical link state algorithm adapted to the necessities of a mobile wireless LAN. The solution notion worn in the protocol is with the intention of multipoint relays (MPRs). MPRs are preferred nodes which forward broadcast messages during the flooding process. This technique substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message.

OLSR works quite well with static nodes. The behaviour is worse when nodes are moving (links are broken). With several hops the protocol has a strange behaviour (interferences or bugs?); the behaviour is different every time the test is performed. Framework improves the performance of protocols running alone. This information is then used for route calculation. OLSR provides optimal routes (in terms of number of hops). The protocol is particularly suitable for large and dense networks as the technique of MPRs works well in this context.

REFERENCE

[1] D. Johnson, Y. Hu, and D. Maltz, “Rfc: 4728,” The dynamic sourc routing protocol (DSR) for mobile ad hoc networks for IPV4, 2007.

[2] C. Perkins and E. Royer, “Ad-hoc on-demand distance vector routing,” in Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA ’99. Second IEEE Workshop on, Feb 1999, pp. 90–100.

[3] F. Hong, L. Hong, and C. Fu, “Secure olsr,” in Advanced Information Networking and Applications, 2005. AINA 2005. 19th International Conference on, vol. 1, March 2005, pp. 713–718 vol.1.

[4] M. Marimuthu and I. Krishnamurthi, “Enhanced olsr for defense against dos attack in ad hoc networks,” Communications and Networks, Journal of, vol. 15, no. 1, pp. 31–37, Feb 2013.

[5] D. Malik, K. Mahajan, and M. Rizvi, “Security for node isolation attack on olsr by modifying mpr selection process,” in Networks Soft Computing (ICNSC), 2014 First International Conference on, Aug 2014,pp. 102–106.