Implementation and Performance Evaluation of Optimized Link State Routing Protocol for Mobile Ad-Hoc Networks.

Mohammed Hesham Ahmed, Usamah Ahmed Khan and Syed Rizwan
Department of Electronics and Communication Engineering,
Muffakham Jah College of Engineering and Technology

***Abstract*—** The Optimized link state routing protocol (OLSR) is a protocol based on the link state algorithm which is pro-active or table driven in nature. OLSR is one of the most suitable routing protocols for the MANETs and it is more vulnerable to black hole attack by the malicious nodes. Hence, a simple yet effective solution to the Black-hole attack is presented. Wireless sensor networks (WSN), are used to cooperatively pass their data through the network to a main location. So a Low-Energy Adaptive Clustering Hierarchy ("LEACH") which is a TDMA-based MAC protocol, is also presented that is integrated with clustering and a simple routing protocol in wireless sensor networks (WSNs). The goal of LEACH is to lower the energy consumption required to create and maintain clusters in order to improve the lifetime of a WSN.

Keywords--

LEACH:	Low Energy Adaptive Cluster Hierarchy
MAC:	Media Access Control
MANET:	Mobile Ad-Hoc Networks
MPR:	Multi-Point Relay
OLSR:	Optimized Link State Route
WSN:	Wireless Sensor Network
TDMA:	Time-Division Multiple Access

I. Introduction

The proliferation of wireless technology in recent years has led to an explosion of research in cost-effective, self-organizing, and efficient wireless technologies for use. Wireless networks allow for high flexibility in setup and relocation, ubiquitous access, and ease of use at the cost of lower throughput (due to interference, a high-loss medium, and limited available spectrum) and weakened security (anyone within range can intercept the signal). The rapid deployment of broadband wireless systems such as 802.11 wireless local area networks (WLANs) (as shown in figure1.1), 802.16 wireless broadband and neighborhood area wireless networks, however, raises concerns in scalability. In short, as networks become larger and denser, capacity issues arise from the inherent broadcast nature of the wireless medium and limited unlicensed spectrum available to use at any given time.

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each device must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).

The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput, ability to scale etc [1].

Optimized Link State Routing (OLSR)

OLSR protocol inherits the stability of link state algorithm. This protocol performs hop-by-hop routing; that is, each node in the network uses its most recent information to route a packet. Hence, even when a node is moving, its packets can be successfully delivered to it, if its speed is such that its movements could at least be followed in its neighborhood. The optimization in the routing is done mainly in two ways. Firstly, OLSR reduces the size of the control packets for a particular node by declaring only a subset of links with the node's neighbors who are its multipoint relay selectors, instead of all links in the network. Secondly, it minimizes flooding of the control traffic by using only the selected nodes, called multipoint relays to disseminate information in the network. As only multipoint relays of a node can retransmit its broadcast messages, this protocol significantly reduces the number of retransmissions in a flooding or broadcast procedure [2].

A. Muti Point Relays

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 symmetric 1-hop neighbors which may retransmit its messages. This set of selected neighbor nodes is called the "Multipoint Relay" (MPR) set of that node [2]. The neighbors of node N which are not in its MPR set receive and process broadcast messages but do not retransmit

broadcast messages received from node N. Each node selects its MPR set from among its 1-hop symmetric neighbors. This set is selected such that it covers all symmetric strict 2-hop nodes. The MPR set of N, denoted as MPR (N), is then an arbitrary subset of the symmetric 1-hop neighbor of N which satisfies the following condition: every node in the symmetric strict 2-hop neighborhood of N must have a symmetric link towards MPR (N). The smaller a MPR set, the less control traffic overhead results from the routing protocol. Each node maintains information about the set of neighbors that have selected it as 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. A broadcast message, intended to be diffused in the whole network, coming from any of the MPR selectors of node N is assumed to here transmitted by node N, if N has not received it yet. This set can change over time and is indicated by the selector nodes in their HELLO messages.

B. Neighbor Detection

Neighbor detection populates the 1-hop neighbor repository and only uses the main addresses of nodes. As seen in the previous section, the neighbor entries are closely related to the link entries. Whenever a link entry is created, the neighbor table is queried for a corresponding neighbor entry. Note that this neighbor entry must be registered on the main address of the node. If no such entry can be located, then a new neighbor entry is created. This means that while a node can have several link-entries describing different links to the same neighbor, only one neighbor entry exists per neighbor.
The status of the neighbor entries is also updated according to changes in the link-set. A neighbor is said to be a symmetric neighbor if there exists at least one link-entry in the link set connecting a local interface to one of the neighbors interfaces where the symmetric timer is not timed out. When a link-entry is deleted, the corresponding neighbor entry is also removed if no other link entries exist for this neighbor.

C. Two Hop Neighbor Detection

A node also maintains a repository of all nodes reachable via symmetric neighbors. This is the two hop neighbor set. This database is used for MPR calculation. Upon receiving a HELLO message from a symmetric neighbor, all reported symmetric neighbors, not including addresses belonging to the local node, are added or updated in the two hop neighbor set. Entries in the two hop neighbor set are all based on main addresses, so for all received entries in the HELLO message the MID set is queried for the main address. Note that the two hop neighbors also may contain neighbors reachable by one hop [3].

D. MPR Selector Detection

The MPR flooding scheme is based on the requirement that nodes have registered what neighbors have chosen them as a MPR. Nodes mark their selected MPR neighbors in HELLO messages by setting the Neighbor Type to be MPR_NEIGH. Upon receiving a HELLO message, a node checks the announced neighbors in the message for entries matching one of the addresses used by the local node. If an entry has a matching address and the neighbor type of that entry is set to MPR_NEIGH, then an entry is updated or created in the MPR selector set using the main address of the sender of the HELLO message.

E. Link State Declaration

Link state routing protocols are based on nodes flooding the network with information about their local links. In protocols like ISIS this information is mostly links to subnets, since these protocols are highly based on aggregation of networks. OLSR uses host based flat routing, so the link state emitted describes links to neighbor nodes. This is done using Topology Control (TC) messages. The format of a TC message is shown in figure. TC messages are flooded using the MPR optimization. This is done on a regular interval, but TC messages are also generated immediately when changes are detected in the MPR selector set. In OLSR the flooding process itself is optimized by the usage of MPRs, but as explained in section, the MPR technique introduces two link-state declaration optimizations as well. As we will see in the Auxiliary functionality chapter, OLSR nodes can also be tuned to send more than just its MPR selector set. One should notice that more robust routing could be achieved by announcing more than the MPR selector set.

C. Black Hole Attacks in MANET

In this type of attacks, malicious node claims having an optimum route to the node whenever it receives RREQ packets, and sends the REPP with highest destination sequence number and minimum hop count value to originator node whose RREQ packets it wants to intercept. For example, in figure 3 when node “S” wants to send data to destination node “D”, it initiates the route discovery process. The malicious node “M” when receives the route request, it immediately sends response to source. If reply from node “M” reaches first to the source than the source node “S” ignores all other reply messages and begin to send packet via route node “M”. As a result, all data packets are consumed or lost at malicious node [4].

D. Resolving the Black Hole Attack

The black-hole attack can be resolved by a simple approach. In this simulation, when no acknowledgment is received by the source node, it immediately senses the black-hole attack taking place and hence chooses to go for an alternate route instead.

E. Hole Detection

In wireless sensor networks (WSNs), certain areas of the monitoring region may have coverage holes and serious coverage overlapping due to the random deployment of sensors. The failure of electronic components, software bugs and destructive agents could lead to the random death of the nodes. Sensors may be dead due to exhaustion of battery power, which may cause the network to be uncovered and disconnected. Based on the deployment nature of the nodes in remote or hostile environments, such as a battle field or desert, it is impossible to recharge or replace the battery. [5] However, the

data gathered by the sensors are highly essential for the analysis, and therefore, the collaborative detection of coverage holes have strategic importance in WSNs. In this paper, distributed coverage hole detection algorithms are designed, where nodes can collaborate to detect the coverage holes autonomously. The performance evaluation of our protocols suggests that our protocols outperform in terms of hole detection time, limited power consumption and control packet overhead to detect holes as compared to other similar protocols.

II. Measurement of Parameters in OLSR, Black-Hole Attack & Resolved Black-Hole Attack

NUMBER OF NODES: 20

PARAMETER	OLSR	BLACKHOLE ATTACK	RESOLVED BH ATTACK
Throughput	619	202.01	474.11
Packet Delivery Ratio	0.353	0.1001	0.248
Packet Density Function	0.9775	0.5211	0.9951
Forward Line	2028	0	1582

NUMBER OF NODES: 30

PARAMETER	OLSR	BLACKHOLE ATTACK	RESOLVED BH ATTACK
Throughput	620.33	212.11	605.21
Packet Delivery Ratio	0.271	0.1012	0.235
Packet Density Function	0.9960	0.4812	0.9964
Forward Line	2122	0	1098

NUMBER OF NODES: 40

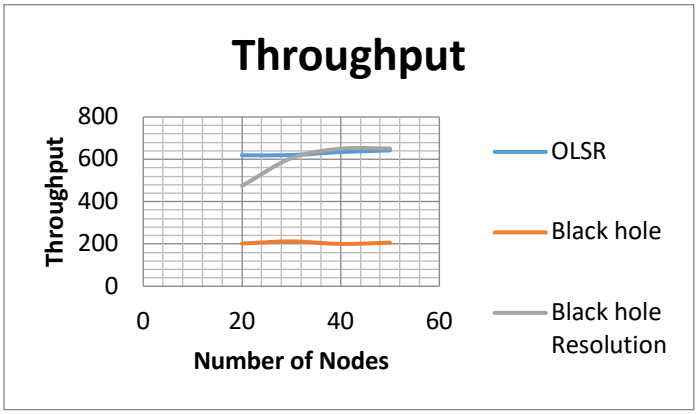
PARAMETER	OLSR	BLACKHOLE ATTACK	RESOLVED BH ATTACK
Throughput	634.47	200.65	650.93
Packet Delivery Ratio	0.391	0.096	0.325
Packet Density Function	0.9963	0.542	0.9967
Forward Line	2021	0	1163

NUMBER OF NODES: 50

PARAMETER	OLSR	BLACKHOLE ATTACK	RESOLVED BH ATTACK
Throughput	642.51	206.21	651.67
Packet Delivery Ratio	0.397	0.1213	0.3912
Packet Density Function	0.9963	0.480	0.9969
Forward Line	2112	0	1005

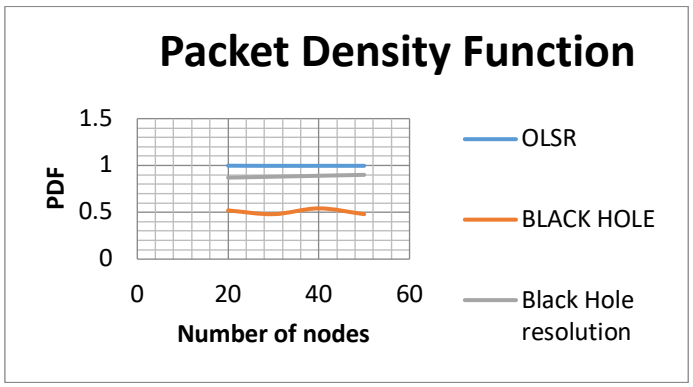
III. Comparison of Parameters

1. Throughput



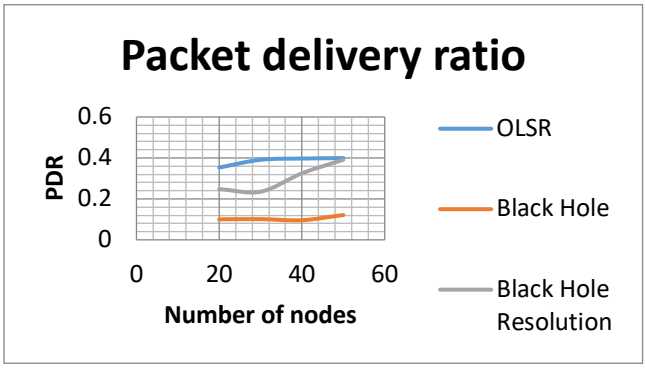
From the graph 5.41 it is seen that the throughput of OLSR is around 630 kbps. But in case of a Black hole attack the throughput of the networks decreases to 200 kbps. In the third case because the black hole is resolved the throughput increases to about 600 kbps.

2. Packet density function



From the graph 5.42 it is seen that the PDF of OLSR is around 0.99. But in case of a Black hole attack the PDF of the networks decreases to 0.50. In the third case because the black hole is resolved the throughput increases to about 0.95.

3. Packet delivery ratio



From the graph 5.42 it is seen that the PDR of OLSR is around 0.35. But in case of a Black hole attack the PDF of the networks decreases to 0.1. In the third case because the black hole is resolved the throughput increases to about 0.3.

REFERENCES

[1] C. Perkins and E. M. Royer. “Ad hoc On-Demand Distance Vector Routing." Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans.

[2] T.Clausen and P. Jacquet. OLSR RFC3626, October 2003. http://ietf.org/rfc/rfc3626.txt

[3] JIRI HOSEK, KAROL MOLNAR; “Investigation on OLSR Routing Protocol Efficiency”, Recent Advances in Computers, Communications, Applied Social Science and Mathematics, ISBN: 978-1-61804-030-5, PP: 147 – 153.

[4] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao “ A survey of black hole attacks in wireless mobile ad hoc networks” Human-centric Computing and Information Sciences 2011.

[5] Li Han, ìLEACH-HPR: An Energy Efficient Routing Algorithm for heterogeneous WSNî IEEE 2010.