OPTIMAL ENERGY-DELAY ROUTING PROTOCOL WITH TRUST LEVELS FOR WIRELESS AD HOC NETWORKS

Eyad Taqieddin (Student), S. Jagannathan (Co-advisor) and Ann Miller (Co-advisor)
Telemetry Learning Center
Department of Electrical and Computer Engineering
University of Missouri-Rolla
Rolla, Missouri 65409
{eyad, sarangap, milleran}@umr.edu

ABSTRACT

An ad hoc network is a group of wireless nodes which do not rely on any fixed infrastructure. Hosts cooperate by forwarding packets for each other to communicate with nodes that are out of the radio transmission range. We propose a new routing algorithm that is based on the concept of multipoint relay nodes (MPR). The main focus of the Trust Level Routing protocol is the reliability and survivability of the network by applying costs to each MPR candidate. The cost calculation is based on the delay incurred, energy available at the MPR node, energy spent during transmission and number of packets sent on each link. We highlight the vulnerabilities in current link state routing algorithms and propose the use of light weight encryption algorithms to achieve a dependable routing algorithm. Network simulator (ns-2) is used to compare the protocol performance to other existing link state routing protocols.

Key words: Routing Protocol, Security, Authentication, Energy, Delay, Wireless Ad hoc Networks, Optimal Route.

I. INTRODUCTION

A Mobile Ad-hoc Network (MANET) is a group of wireless mobile nodes that form a dynamic network topology without any centralized administration or fixed infrastructure. The nodes mobility requires establishing and breaking connections whenever needed. Each node communicates directly with the nodes within its wireless range. However, the nodes need to collaborate together to deliver the information between nodes that are beyond the wireless range of the source.

With this approach, in terms of transmission, each node operates in two modes; source or relay. Source nodes generate the traffic on the network whereas relay nodes receive the packets and forward them to the intended destination.

A routing protocol is used to detect the topology of the network and to enable each node to have

a path to any of its intended destinations. The nodes share information among each other to build their respective routing tables and to report any changes in network topology. This is usually done using control packets as will be discussed later. This, however, lies on the assumption that the contents of the received packets are authentic.

The lack of authentication detection can be a serious hazard to the proper operation of the routing protocol. Malicious nodes can send incorrect information in the control packet to cause a denial of service or loops in the network.

The rest of this paper is organized as follows: Section II discusses the Optimized Link-State Routing (OLSR) and the Optimized Energy-Delay Routing (OEDR) protocols. Section III highlights the vulnerabilities and security threats. In section IV, we present the Trust Level Routing protocol (TLR). Section V presents the results obtained using the ns-2 simulations and Section VI presents the conclusions and future directions.

II. OVERVIEW OF OLSR & OEDR

OLSR and OEDR are proactive link state routing protocols. Their operation is table driven through periodically exchanging topology information with other nodes in the network.

The main objective of these protocols is to minimize the effect of flooding which usually happens when all the nodes in the network forward very control packet received. As a result, multiple copies of the same control packet will be delivered.

A solution for this problem is to designate Multipoint Relay (MPR) nodes. Upon reception of a control packet, an MPR forwards it to its neighbors whereas non-MPR nodes that receive the same packet do not route it to the designated next hop. This results in better usage of the available bandwidth and less congestion in the network.

There are two types of packets used for selecting the MPRs and constructing the routing tables.

- Hello packets

  Each node broadcasts Hello packets to the neighbors within its range of transmission. In OLSR, the Hello packet contains fields for the address of the originator, information about the neighbors' link status, and a list of nodes selected as MPRs for the originator. The recipients of the Hello packets add the originator into the 1-hop neighbor table.

  When a node receives a Hello message, it implicitly learns about its two 2-hop neighbors. This information, which is essential for the MPR selection, is stored in a 2-hop neighbor table.

  Hello packets in OEDR contain the same fields in addition to the transmission time (used for calculating the delay), transmission energy, and the available energy of the source node. This additional information is stored in the 1-hop neighbor table.

- Topology Control (TC) packets

  These packets are used to propagate the topology information throughout the network. Each node includes its address, a list of the selected MPRs and a sequence number to avoid creating loops. TC packets are only forwarded by the MPRs.

MPR selection

In OLSR, MPRs are selected from the one hop neighbors such that all two hop neighbors will receive the data packets through one of the MPRs. The basis of selection is to choose the smallest set of MPR nodes to fully cover all the 2-hop neighbors.

OEDR, on the other hand, bases the selection on minimizing the energy-delay cost to reach the two hop neighbors. Furthermore, the amount of energy available in a node is a factor in the cost calculation (i.e. nodes with lower power will have higher link costs).

Based on that, the MPR set chosen by OLSR does not necessarily have to be the same for that of OEDR. Moreover, if the nodes are static, the MPR set for nodes running OLSR will always be the same unless one of more nodes loses their battery power. In OEDR, the MPR set is dynamically changed based on the factors above.

As mentioned earlier, a Hello packet contains a list of the MPRs selected by the originator. When such a packet is received, it adds the originator to its MPR Selectors table. This table is used whenever a TC packet is received to determine if it should be relayed (originator in selectors table) or not.

III. SECURITY THREATS

The OLSR and OEDR algorithms do not provide any security measures to guarantee the confidentiality of the data transmission and proper routing. Because of this, malicious nodes can perform a variety of attacks to obstruct the communication on the network.

Passive Attack

In this form of attack, a node resides within the communication range of one of the MPR nodes. By doing so, it can capture all the information sent from the source node and use that information for future off line analysis.

Our proposed algorithm limits the effect of this attack by using the number of packets sent through each MPR, along with the energy and delay, as a factor in calculating the cost of the link. As a result, with every packet sent on a link, the cost of that link will increase until we reach a point where another link has a lower cost and the routing tables are updated to use a different MPR.

Active Attacks

- Hello attack

  In this attack, a malicious node repeatedly sends hello packets to its neighbors with inconsistent information. This forces other nodes to spend a relatively large percentage of their energy on processing the received Hello packets and updating their tables.

  Another variant of this attack is when a malicious node has a long transmission range compared to other nodes on the network. It could transmit a Hello packet that reaches all the nodes thus adding itself to the neighbor table of each node and causing incorrect routing information to be relayed between the nodes.

- Impersonation

  Since no authentication takes place, a malicious node can masquerade as another node (spoofing). A spoofing node can generate false Hello or TC packets to cause a change in the routing tables of the nodes. This could lead to routing loops or denial of service.

- Inducement

  As mentioned earlier, OEDR link cost calculation depends on the delay, energy used for the transmission on the link, and the reciprocal of remaining energy in the MPR candidate. An adversary sends a Hello packet showing that it has a large amount of energy remaining in its battery. This misleads the sending node to calculate a low cost for the link and thus selects the malicious node as the MPR. At this point, all the traffic is going through this node and it can either drop the packets (denial of service), selectively forward packets, or simply forward all the packets while storing copies for future offline analysis.

- Modification

  MPR nodes are responsible for forwarding the packets to other nodes. While doing that task, a malicious MPR may change the payload or even change the destination field before transmitting the packet to the next hop. Another form of modification is to change the packet sequence number to match one what was previously used, resulting in a packet drop.

- Energy drain attack

  Two malicious nodes with high energy can drain the energy of a third node by positioning themselves around it and using it as an MPR. They can transmit packets repeatedly through that node until its energy is depleted.

VI. TRUST LEVELS IMPLEMENTATION

With the vulnerabilities listed in the previous section, it is clear that the operation of OLSR and OEDR would become ineffective in the presence of malicious nodes. For that purpose, an extension of the OEDR protocol called the Trust Level Routing (TLR) protocol is suggested.

In this work, we propose two methods for adding trust levels in the routing protocol: load balancing and authentication.

Load balancing

In this method, the traffic going from source A to destination B is routed through different paths by continuously switching between MPRs. This denies any malicious node in the intermediate path the chance to capture the whole stream of data.

In OEDR, the cost of a direct link between nodes x and y is defined as

$C_{x,y}$ = Energy [x->y] * Delay [x->y] (1)

Moreover, the cost for selecting node n1 as an MPR to reach a two hop neighbor n2 is given by

$$C^{MPR}_{s,n_1,n_2} = C_{s,n_1} + C_{n_1,n_2} + (1 / E_{n_1}) \quad (2)$$

Where E_{n1} = Energy available in node n1 (i.e. the MPR candidate).

Our proposed approach is based on incorporating the number of packet sent through a neighbor in the cost calculation. Thus, the cost for any direct link becomes

$C_{x,y}$ = Energy [x->y] * Delay [x->y] + w_1 * No. of packets[x->y] (3)

Where w_1 is a weight factor that depends on the data rate of the nodes.

From equation (3), it is evident that as the number of data packets increases on a certain link, the cost of using that link will increase until the total cost in (2) becomes higher than that of another link. At this point, the MPR list of the source will be updated to force a route change.

To simulate the protocol modifications, the ns-2 implementation of OEDR was extended to reflect the changes in cost calculation. A new table was added in each node to hold the number of packets sent on each link.

The simulation scenarios were based on networks of 50 and 200 nodes. The data rates varied from 128 kbps to 4096 kbps with a packet size of 512 bytes. The nodes were stationary in an area of 1000 x 1000 meters, their locations and flows were randomly generated. The performance of the three routing protocols was compared based on the end-to-end delay and the energy-delay product.

Figures 1 and 2 show the average end-to-end delay for data packets on networks of 50 and 200 nodes, respectively. The delay in TLR is similar to that of OEDR. In some cases, however, it is less and that is due to the implicit contention avoidance in TLR. When a sequence of packets is sent through a path, the contention in the intermediate nodes will increase. Since TLR sends data through different paths, it avoids causing contention in the intermediate nodes, thus reducing the average delay.

The figures also show that the delay for OLSR is higher; this is because OEDR and TLR consider the delay as a factor in choosing the routes whereas OLSR just selects the smallest set of possible MPRs.

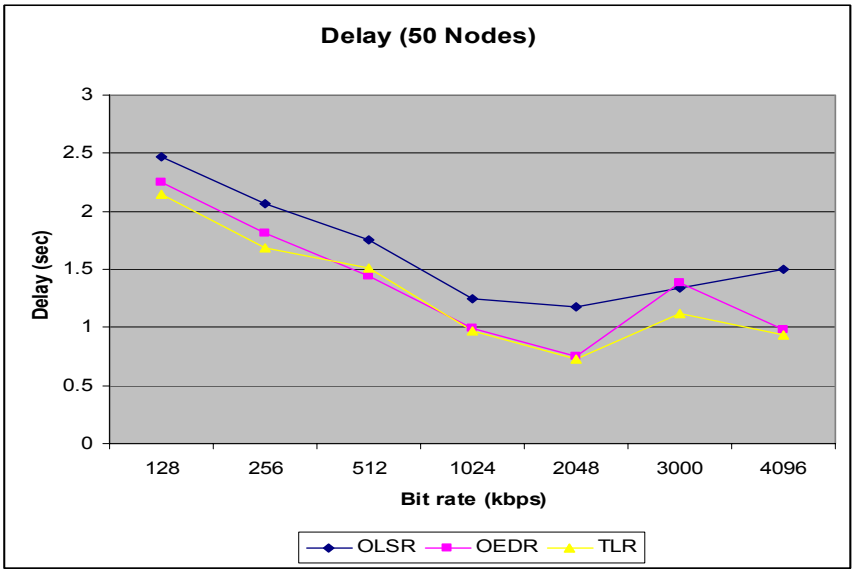

Figure 1. Delay for the three routing protocols in a 50 node network

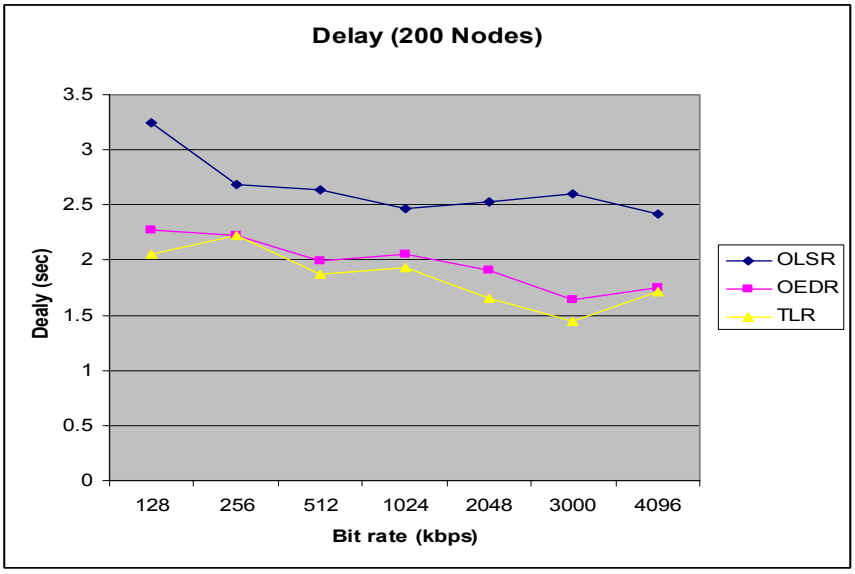

Figure 2. Delay for the three routing protocols in a 200 node network

In Figures 3 and 4, the energy-delay per packet is given for networks of 50 and 200 nodes, respectively. OLSR always has a higher energy-delay product compared to OEDR and TLR. From the figures, we also notice that OEDR performs better in terms of this metric. This is explained by the introduction of the packet count as a metric which forces the nodes to select some MPR nodes that are not optimal in terms of energy consumption and the link delay.

By comparing Figures 3 and 4, we find that the energy-delay metric increases as the number of nodes increases. This is due to the higher amount of traffic flowing in the network and use of different path with more intermediate hops (i.e. more energy consumption).

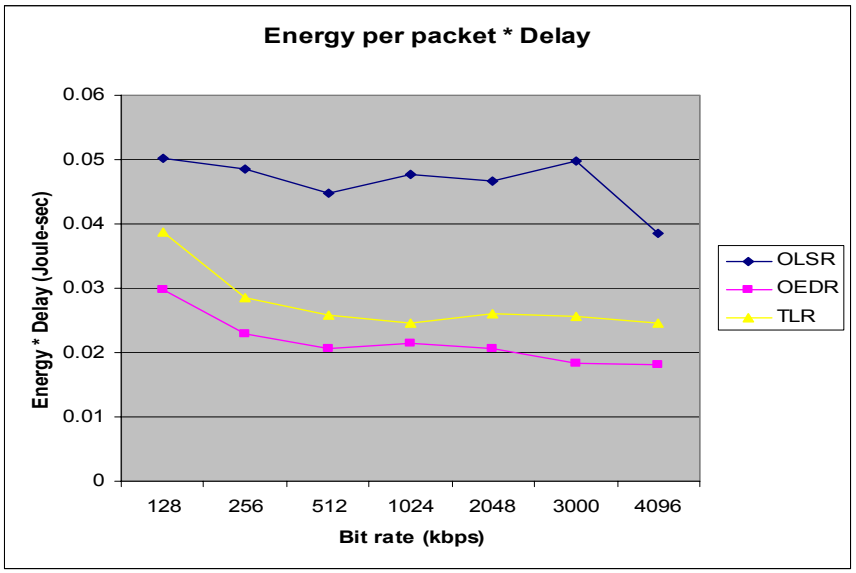

Figure 3. Delay for the three routing protocols in a 200 node network

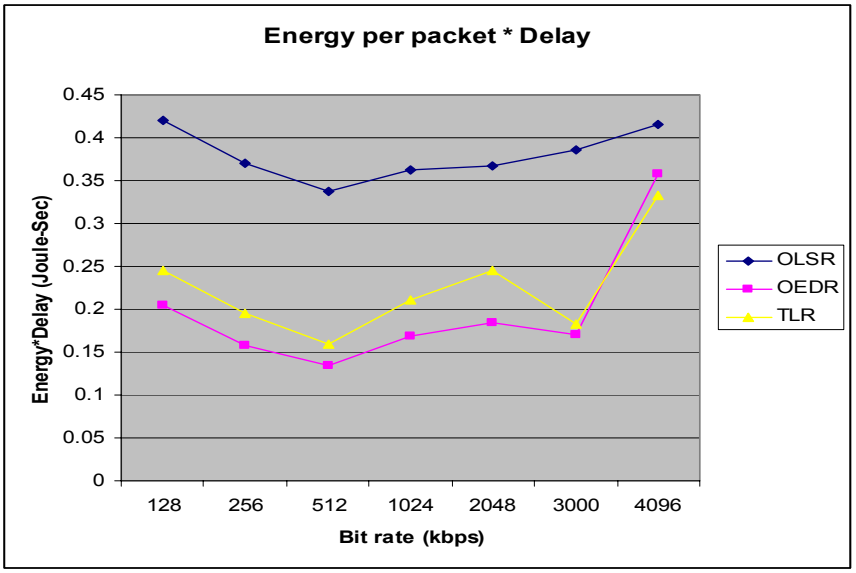

Figure 4. Delay for the three routing protocols in a 200 node network

Authentication and timestamps

Load balancing provides a reasonable level of security when combined with a lightweight encryption algorithm. It is helpful in reducing the risk of passive attacks but has little potential in overcoming or even detecting active attacks.

Authentication of the control packet source can be used to counter active attacks. Assuming that the authentic nodes in the network have a mechanism for sharing the encryption keys and they all share a one way hash function. Node A uses the shared key and the contents of the control packet to calculate a hash code which is inserted as a field in the control packet itself. When node B receives the packet, it applies the hash function on the secret key and the body of the received packet (excluding the hash field) to calculate the hash code. By comparing the result with the hash field of the packet, the node determines whether the message is authentic or not.

Assuming that a malicious node alters the message but does not alter the hash code (because it does not have the secret key), then node B can easily detect the changes in the packet and drop it.

This guarantees that the packet was sent by one of the authentic nodes because only they have the shared key and that the payload of the control packet was not changed in transit

The scheme above, by itself, is not enough for authentication. Consider a scenario where node A sends control messages to node B. Assuming that a malicious node M intercepts the control message, it could wait for a random period and then retransmit the same packet. When node B receives the replayed message, it checks the hash code and accepts the packet as authentic. This will cause inconsistencies in the routing table of node B.

Timestamps can be used to overcome this problem. Whenever a node sends a packet, it adds the time of transmission as a field and includes that in the hash calculation. This enables the recipients to check the time of transmission.

Only Hello packets in OEDR contain the time of transmission. TC packets need to be modified to include this field to avoid the replay attack.

The OEDR implementation in ns-2 was modified by adding definitions for the malicious nodes and providing a mechanism for authentication. Every packet received is checked in the MAC layer, and any packet from a non-authentic source is dropped. This means that no entries will be added in the one-hop or two hop tables. Thus, the malicious nodes will not be qualified to be MPRs.

A network of 50 nodes is tested first in an “attack-free” environment where all the nodes are authentic. Then the same network is simulated in the presence of 5 malicious nodes. Figure 5 shows the increase of the drop rate with the inclusion of non-authentic nodes increases.

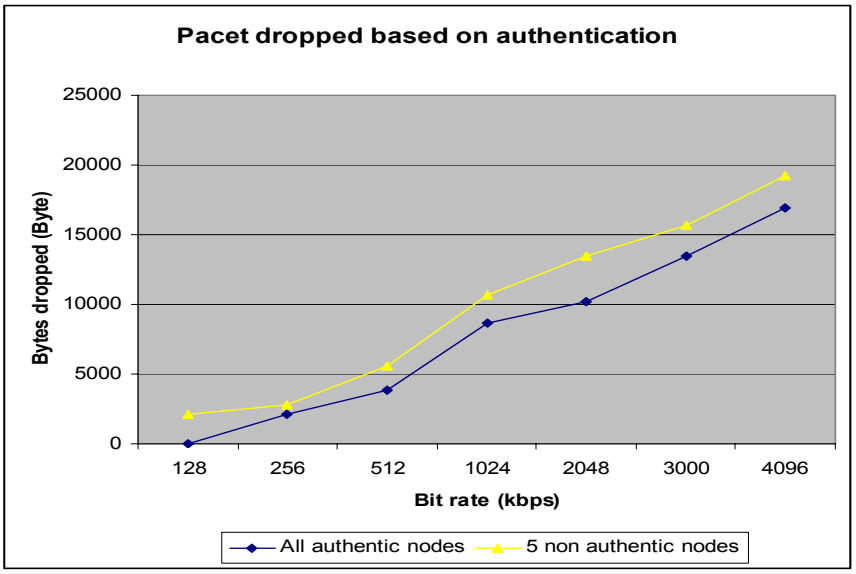

Figure 5. Packets dropped in two scenarios for test network

VI. CONCLUSIONS AND FUTURE DIRECTIONS

With the rapid deployment of wireless networks, security of the routing protocols is essential for reliable operation. The threats presented in this paper indicate that much work is needed to guarantee the privacy and integrity of the data. This is especially important in military and safety critical environments.

TLR, an extension of the OEDR protocol, resulted in better management of route selection for security purposes. The simulation results indicate that TLR delivered the packets with a noticeable decrease in the average end-to-end delay. This, however, increased the power consumed when longer routes were selected.

The addition of the authentication model in ns-2 demonstrated how the TLR protocol dropped non-authentic control packets. Nevertheless, more work needs to be done to improve the model to enable the analysis of the computational overhead involved in computing the hash fields as well as the bandwidth utilized for the additional bytes inserted into the control packet in the form of the hash code.

Another modification to be investigated is the weight calculation equation given in (3). A dynamic model that allows assigning different weights to each factor would be more suitable in cases where, for example, delay is given higher priority than energy consumption.

VI. REFERENCES

[1] Jacquet, P., Muhlethaler, P., Clausen, Thomas, Laouiti, A., Qayyum, A., and Viennot, L., "Optimized link state routing protocol for ad hoc networks", pp. 62 – 68,IEEE International

Multi Topic Conference on Technology for the 21st Century, IEEE INMIC'01, December, 2001.

[2] Qayyum, A., Viennot, L., and Laouiti, A. "Multipoint relaying for flooding broadcast messages in mobile wireless networks", pp. 3866 – 3875, 35th Annual Hawaii International Conference on System Sciences, HICSS, January, 2002.

[3] Regatte, N. and Sarangapani, Jagannathan, "Optimized Energy-Delay Routing in Ad Hoc Wireless Networks", Proceedings of World Wireless Conference, San Francisco, CA, May, 2005.

[4] Adjih, C., Clausen, Thomas, Jacquet, P., Laouiti, A., Muhlethaler, P., and Raffo, D., "Securing the OLSR Protocol", Proceedings of Med-Hoc-Net, Mahdia, Tunisia, June, 2003

[5] Michiardi, P. and Molve, R. "Simulation-based Analysis of Security Exposures in Mobile Ad Hoc Networks", European Wireless Conference, 2002.

[6] Rawat, K. and Massiha, G., "Secure Data Transmission Over Wireless Networks: Issues and Challenges", IEEE Region 5, 2003 Annual Technical Conference, 2003

[7] Dahill, B., Levine, B., Royer, E. and Shields, C., "A Secure Routing Protocol for Ad Hoc Networks", Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan, August, 2001.