ISSN:0975-9646

Collaborative Scheme to Detect Stealth Nodes in Mobile Adhoc Networks

Burra Naga Durga Srinivas, M.V.S.S. Nagendranath

Department of CSE
SASI Institute of Technology and Engineering
Tadepalligudem,Andhrapradesh, India

***Abstract*— Limited number of nodes are static in Mobile Adhoc Networks. Hence achieving synchronization between neighboring nodes in such a dynamic environment is complicated considering issues like signal disruptions, transmission power variations, loss of communication. Earlier a simple protocol that uses a continuous neighbor discovery algorithm through neighbor collaboration was deployed. Besides its ability to address the above issues it can detect hidden nodes that are detrimental to quality and security. Precise knowledge of node localization is important for robust communications in MANETs. So we propose to use the above protocol with a centralized node localization scheme to improve overall efficiency.**

I.INTRODUCTION

A **mobile ad-hoc network** (**MANET**) is a self-configuring infrastructure less network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. When any two nodes want to communicate then both must be in active state.

The nodes are placed randomly over the area of interest and their first step is to detect their immediate neighbors , the nodes with which they have a direct wireless communication and to establish routes to the gateway. In heavy traffic networks, there is no need to invoke neighbor discovery protocol. This is because any new node, or a node that has lost connectivity to its neighbors, can hear its neighbors simply by listening to the channel for a short time. The nodes must continuously look for new neighbors in order to accommodate the following situations:

1) Loss of local synchronization due to accumulated clock drifts.

2) Disruption of wireless connectivity between adjacent nodes by a temporary event. When these events are over, the hidden nodes must be rediscovered.

(3)The ongoing addition of new nodes, in some networks to compensate for nodes which have ceased to function because their energy has been exhausted.

4) The increase in transmission power of some nodes, in response to certain events, such as detection of emergent situations.

For these reasons, detecting new links and nodes in networks must be considered as an ongoing process. In the following discussion we distinguish between the detection of new links and nodes during initialization, i.e., when the node is in Init state, and their detection during normal operation, when the node is in Normal state. The former will be referred to as *initial neighbor discovery* whereas the latter will be referred to as *continuous neighbor discovery.* A node in the Init state is also referred as a hidden node and a node in the Normal state is referred to as a segment node. When node u is in the Init state, it performs initial neighbor discovery. After a certain time period, during which the node is expected, with high probability, to find most of its neighbors, the node moves to the Normal state, where continuous neighbor discovery is performed.

To perform continuous neighbor discovery, we implemented OLSR, a proactive routing protocol, which is an optimization version of a pure link state protocol in which the topological changes cause the flooding of the topological information to all available hosts in the network. Implementation of OLSR protocol is specified in section IV and performance is specified in section V.

II.RELATED WORK

In a WiFi network operating in centralized mode, a special node, called an access point, coordinates access to the shared medium. Messages are transmitted only to or from the access point. Therefore, neighbor discovery is the process of having a new node detected by the base station. Since energy consumption is not a concern for the base station, discovering new nodes is rather easy. The main differences between neighbor discovery in WiFi and in mesh sensor networks are that neighbor discovery in the former are performed only by the central node, for which energy consumption is not a concern. In addition, the hidden nodes are assumed to be able to hear the HELLO messages broadcast by the central node. In contrast, neighbor discovery in sensor networks is performed by every node, and hidden nodes cannot hear the HELLO messages when they sleep. In mobile ad-hoc networks (MANETs), nodes usually do not switch to a special sleep state. Therefore, two neighboring nodes can send messages to each other whenever their physical distance allows communication. AODV [9] is a typical routing protocol for MANETs. In AODV, when a node wishes to send a message to another node, it broadcasts a special RREQ (route request) message. This message is then broadcast by every node that hears it for the first

time. The same message is used for connectivity management, as part of an established route maintenance procedure, aside from which there is no special neighbor discovery protocol.

III. PROBLEM DEFINITION

Two nodes are said to be neighboring nodes if they have direct wireless connectivity. We assume that all nodes have the same transmission range, which means that connectivity is always bidirectional. A set of connected nodes is referred to as a segment. Consider a pair of neighboring nodes that belong to the same segment but are not aware that they have direct wireless connectivity. These two nodes can learn about their hidden wireless link using the following simple scheme, which uses a message types: (a) SYNC messages for synchronization between all segment nodes, transmitted over known wireless links; (b) HELLO messages for detecting new neighbors.

D*etecting all hidden links inside a segment:* This scheme is invoked when a new node is discovered by one of the segment nodes. The discovering node issues a special SYNC message to all segment members and periodically broadcast a bunch of HELLO messages. This SYNC message is distributed over the already known wireless links of the segment. Thus, it is guaranteed to be received by every segment node. When Scheme is used, a hidden node is discovered by all of its neighbors as soon as it is discovered by the first of them.

IV. COMPARISON OF REACTIVE AND PROACTIVE ROUTING PROTOCOLS

Reactive Protocols: Reactive routing is also known as on-demand routing protocol since they don't maintain routing information or routing activity at the network nodes if there is no communication. These protocols take a lazy approach to routing. They do not maintain or constantly update their route tables with the latest route topology. If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packet. The route discovery usually occurs by flooding the route request packets throughout the network. Examples of reactive routing protocols are the dynamic source Routing (DSR), ad hoc on-demand distance vector routing (AODV).

Proactive Protocols: These routing protocols are similar to and come as a natural extension of those for the wired networks. In proactive routing, each node has one or more tables that contain the

latest information of the routes to any node in the network. Each row has the next hop for reaching a node/subnet and the cost of this route. Various table-driven protocols differ in the way the information about a change in topology is propagated through all nodes in the network. There exist some differences

Protocol Property	**DSDV**	**DSR**	**AODV**	**OLSR**
Multicast Routes	No	Yes	No	Yes
Distributed	Yes	Yes	Yes	Yes
Unidirectional Link Support	No	Yes	No	Yes
Multicast	No	No	Yes	Yes
Periodic Broadcast	Yes	No	Yes	Yes
QoS Support	No	No	No	Yes
RoutesMaintained	Route in Table	Route Cache	Route Table	Route Table
Protocol	Proactive	Reactive	Reactive	Proactive

Table : Characteristics comparison of protocols

between the protocols that come under this category depending on the routing information being updated in each routing table. Furthermore, these routing protocols maintain different number of tables. The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table

leading to consumption of more bandwidth. Examples of such schemes are the conventional routing schemes, Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing(OLSR).

V. AN EFFICIENT CONTINUOUS NEIGHBOR DISCOVERY ALGORITHM : OLSR

For neighbor discovery, Optimized link state routing protocol was implemented. OLSR is a table – driven pro-active that contains a continuous control traffic by the routers. All the time topology information about the network is exchanged by the node regular. To minimize the overhead of flooding messages in the network, OLSR uses the method of multipoint relays (MPR). To detect neighbors the OLSR broadcasts periodically HELLO messages into the network.

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 neighbors. With the Hello message the Multipoint Relay (MPR) Selector set is constructed which describes which neighbors 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. TC messages are used for broadcasting information about own advertised neighbors which includes at least the MPR Selector list. The TC messages are broadcasted periodically and only the MPR hosts can forward the TC messages.

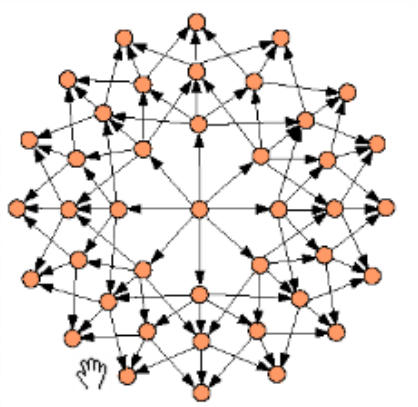

Fig: broadcast flooding in network.

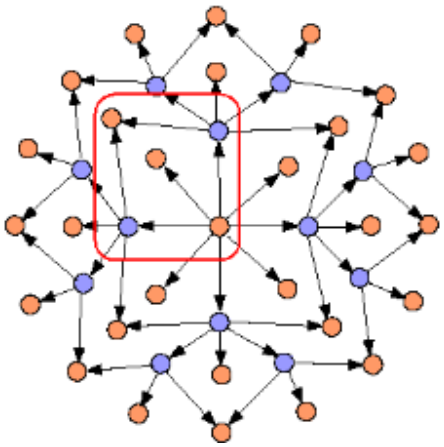

Fig : overhead reduced by MPR.

The link in the ad hoc network can be either unidirectional or bidirectional so the host must know this information about the neighbors. The Hello messages are broadcasted periodically for the neighbor sensing. The Hello messages are only broadcasted one hop away so that they are not
forwarded further. When the first host receives the Hello message from the second host, it sets the second host status to asymmetric in the outing table. When the first host sends a Hello message and includes that, it has the link to the second host as asymmetric, the second host set first host status to symmetric in own routing table. Finally, when
second host send again Hello message, where the status of the link for the first host is indicated as symmetric, then first host changes the status from asymmetric to symmetric. In the end both hosts knows that their neighbor is alive and the corresponding link is bidirectional.
The Hello messages are used for getting the information about local links and neighbors. The Hello messages periodic broadcasting is used for link sensing, neighbor's detection and MPR selection process. Hello message contains: information how often the host sends Hello messages, willingness of host to act as a Multipoint Relay, and information about its neighbor. Information about the neighbors contains: interface address, link type and
neighbor type. The link type indicates that the link is symmetric, asymmetric or simply lost. The neighbor type is just symmetric, MPR or not a neighbor. The MPR type indicates that the link to the neighbor is symmetric and that this host has chosen it as Multipoint Relay.
The host maintains the routing table, the routing table entries have following information: destination address, next address, number of hops to the destination and local interface address. Next address indicates the next hop host. The information is got from the topological set (from the TC messages) and from the local link information base
(from the Hello messages). So if any changes occur in these sets, then the routing table is recalculated. Because this is proactive protocol then the routing table must have routes for all available hosts in the network. The information about broken links or partially known links is not stored in the routing table.
The routing table is changed if the changes occur in the following cases: neighbor link appear or disappear, two hops neighbor is created or removed, topological link is appeared or lost or when the multiple interface association information changes. But the update of this information does not lead to the sending of the messages into the network. For finding the routes for the routing table entry the shortest path algorithm is used.

VI PERFORMANCE ISSUE

In the figures presented here, OLSR-DEF refers to the default values of OLSR *Hello* and *TC* message intervals which are 2 and 5 seconds respectively. In OLSR-MOD these values are changed to 1 and 3 seconds respectively. Figure 1 and Figure 2 show the average percentage of PDR against communication sessions and number of nodes. In Figure 1 we observe that the packet delivery ratio of OLSR-MOD is consistently more than both OLSR-DEF and AODV. OLSR-DEF performs slightly better than AODV but it may not be suitable in place of AODV as its routing overload will be much higher than AODV. OLSR performs better with short *Hello* and *TC* message intervals. It is an important result, because with these short values OLSR is better equipped to cope with the rapidly changing and highly dynamic topology of MANET where link are often short live. Figure 2 shows the PDR against node density. Here again we see that OLSR-MOD performs better than AODV and OLSR-DEF by a slight margin. As the network size increases, with more nodes in it, the proactive routing protocol is able to perform better than the reactive routing protocol.

Figure 3 and 4 show the average End-to-End delay against both communication sessions and node density. In figure 3 we see that although average end-to-end delay of AODV is steady, but it is always more than OLSR-MOD. Similar observation can be made when node density

increases. Here again proactive routing protocol performs better than reactive routing protocol.

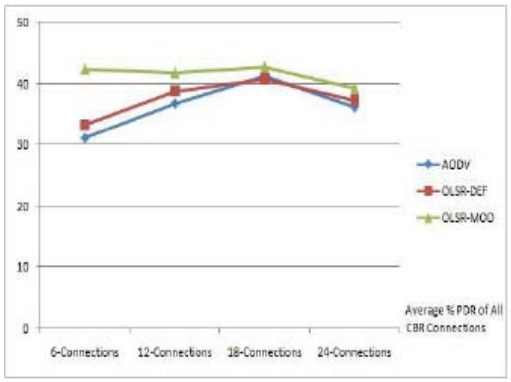

Fig. 1. Packet Delivery Ratio vs. Communication Sessions

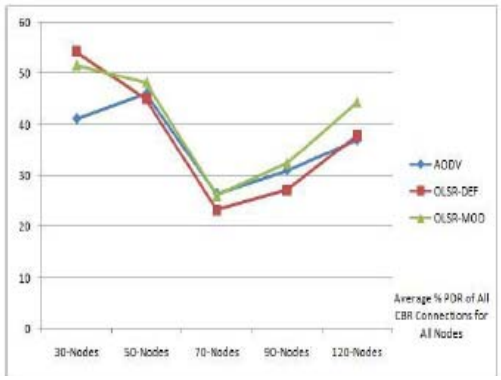

Fig. 2. Packet Deliver Ratio vs. Node Density

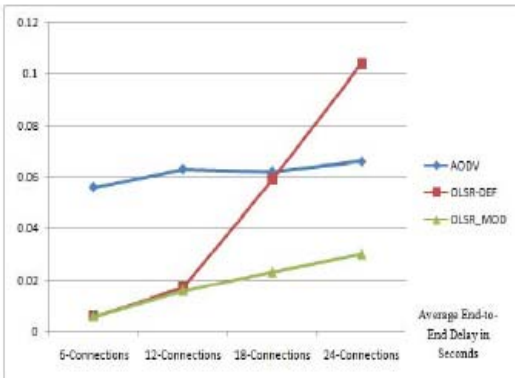

Fig. 3. Avg. End-to-End Delay vs. Communication Sessions

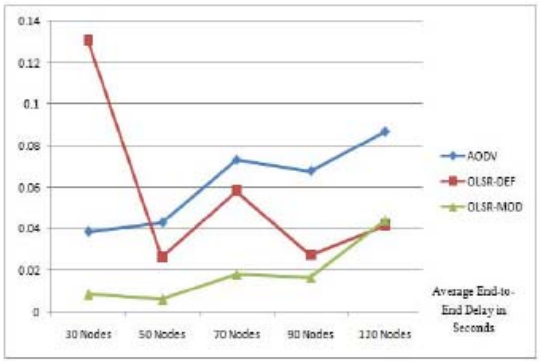

Fig. 4. Avg. End-to-End Delay vs. Node Density

VII CONCLUSION

For efficient neighbor discovery , OLSR protocol is proposed. OLSR protocol is implemented to address different aspects like loss of communication , transmission delay , signal interruption . OLSR keeps track of routing table in order to provide a route if needed. OLSR can be implemented in any ad hoc network. Due to its nature OLSR is called as proactive routing protocol. OLSR routing protocol is capable to manage thousand nodes. MPRs report only its selector table, i.e., the nodes that the selected the sender node as its MPR. Selecting the MPR sets as small as possible ensure overhead of the protocol is kept at minimum. In performance evaluation two variants of OLSR were tested, one with default interval values of *Hello* and *TC* messages and other with short interval values of these messages. OLSR with more frequent *Hello* and *TC* messages was able to give better PDR and less End-to-End delay than AODV and its default variant.

VIII REFERENCES

[1] Phillipi schult –hedicamp, “Mobil network routing with OLSR”.

[2] P.Jacquet, P.Muhlethaler, T.clausen, A.Laouiti, A.Qayyam , L.Viennot ,”Optimized link state routing in mobile adhoc networks”.

[3] Aleksandr Huhtonen, “Comparing AODV and OLSR Routing Protocols.”

[4] Laurent Ouakil, Sidi-mohammed senouki , Guy pujoli, “Performance Comparison of Ad Hoc Routing Protocols Based on Energy Consumption .“

[5] M. J. McGlynn and S. A. Borbash, .Birthday protocols for low energy deployment and _exible neighbor discovery in ad hoc wireless networks,. in MobiHoc: Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York, NY, USA: ACM Press, 2001, pp. 137.145.

[6] C. Perkins, E. Belding-Royer, and S. Das, .Ad hoc on-demand distance vector (AODV) routing,. RFC 3561, July 2003