International Journal of Networking
ISSN: 2249-278X & E-ISSN: 2249-2798, Volume 2, Issue 1, 2012, pp.-35-39.
Available online at http://www.bioinfo.in/contents.php?id=108

A REVIEW PAPER ON ROUTING PROTOCOLS OF WIRELESS AD-HOC NETWORK TECHNOLOGY

THAKARE P.P., JOSHI M.A. AND RAUT A.D.

Department of Computer Science, Jawaharlal Darda Institute of Engineering & Technology, Yavatmal, MS, India.
*Corresponding Author: Email- mayurijoshi5692@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- Ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. ad hoc networking offers convenient infrastructure-free communication over the shared wireless channel. This research paper provides an overview of these protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. This study experimentally compares the performance of three different multi hop ad hoc network routing protocols. Traditional routing protocols have proven inadequate in wireless ad hoc networks, motivating the need for ad hoc specific routing protocols. This study tests link state, distance vector and biologically inspired approaches to routing using OLSR, Babel and BATMAN routing protocols. The importance of OSI layers is also discussed. This study concludes that the routing protocol's overhead is the largest determinant of performance in small multi hop ad hoc networks. The results show that Babel outperforms OLSR and BATMAN routing protocols and that the OSI layer of the routing protocol has little impact on performance

Keywords- Ad hoc, Multi hop, Babel, Clustering/hierarchical routing, Batman, Partial Mesh

Citation: Thakare P.P., Joshi M.A. and Rout A.D. (2012) A review paper on routing protocols of wireless ad-hoc network technology. International Journal of Networking, ISSN: 2249-278X & E-ISSN: 2249-2798, Volume 2, Issue 1, pp.-35-39.

Introduction

Wireless Ad-hoc Networks operates without a fixed infrastructure. Multi-hop, mobility, large network size combined with device heterogeneity and bandwidth and battery power limitations, all these factors make the design of routing protocols a major challenge. Lots of researchers did tremendous work on the Wireless Ad-hoc Routing Protocols. Wireless networks allow hosts to roam without the constraints of wired connections. People can deploy a wireless network easily and quickly. End users can move around while staying connected to the network. Wireless networks play an important role in both military and civilian systems. Handheld personal computer connectivity, notebook computer connectivity, vehicle and ship networks, and rapidly deployed emergency networks are all applications of this kind of network. Hosts and routers in a wireless network can move around. Therefore, the network topology can be dynamic and unpredictable.

Traditional routing protocols used for wired networks cannot be directly applied to most wireless networks because some common assumptions are not valid in this kind of dynamic network. For example, one assumption is that a node can receive any broadcast message sent by others in the same subnet. However, this may not be true for nodes in a wireless mobile network. The bandwidth in this kind of network is usually limited. Thus, this network model introduces great challenges for routing protocols.

Traditional Techniques

Traditionally, the nodes employ routing tables in order to perform the forwarding of packets they receive. Each node knows the next hop to send a packet on the route to its destination. The routing tables are set up automatically using routing protocols which take a few seconds to converge. AODV is an example of such a protocol.

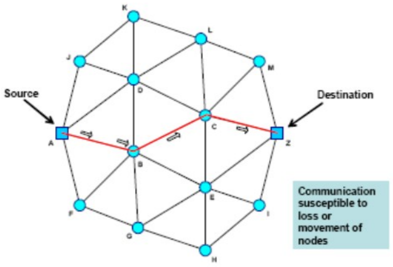

Fig. 1- Partial Mesh with Hop by Hop Forwarding

However, if one of the nodes on a path moves out of range of its neighbors or becomes disabled, or if communication conditions along part of a path degrade, a break in the hop-by-hop forwarding path occurs and the packet flow is interrupted.

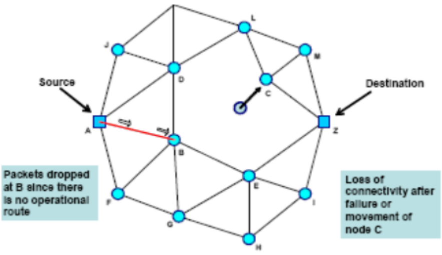
L
J
M
D
Source
C
Destination
A
Z
B
Packets dropped at B since there is no operational route
E
Loss of connectivity after failure or movement of node C
F
I
G
H

Fig. 2- Disrupted Hop-by-hop Forwarding

If an alternative route is available, the routing protocol will find it and the routing tables will be adjusted, but this will take a few seconds during which time packets will be lost (Figure 3). This makes traditional routed networks unsuitable for real-time and mission critical communications.

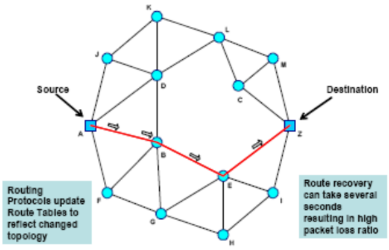
K
L
J
M
D
Source
Destination
C
A
Z
B
E
Routing Protocols update Route Tables to reflect changed topology
Route recovery can take several seconds resulting in high packet loss ratio
F
I
G
H

Fig. 3- Route Table Update

This study experimentally compares the performance of three different multi hop ad hoc network routing protocols. Traditional routing protocols have proven inadequate in wireless ad hoc networks, motivating the need for ad hoc septic routing protocols. This study concludes that the routing protocol's overhead is the largest determinant of performance in small multi hop ad hoc networks.

Type of Protocol

A. Table-driven routing protocols-

Based on the periodically exchanging of routing information between the different nodes, each node builds its own routing table which it can use to find a path to a destination[12]. Examples of the protocols of this class are, Destination Sequenced Distance Vector routing protocol (DSDV), Wireless Routing Protocol (WRP), Cluster-Head Gateway Switch Routing protocol and Source Tree Adaptive Routing protocol (STAR).

B.A.T.M.A.N.

B.A.T.M.A.N. detects the presence of B.A.T.M.A.N.-Originators, no matter whether the communication path to/from an Originator is a single-hop or multi-hop communication link. The protocol does not try to find out the full routing path; instead it only learns which link-local neighbor is the best gateway to each Originator. It also keeps track of new Originators and informs its neighbors about their existence. The protocol ensures that a route consists of bidirectional links only.

On a regular basis every node broadcasts an originator message (or OGM), thereby informing its link-local neighbors about its existence (first step). Link-local neighbors which are receiving the Originator messages are relaying them by rebroadcasting it, according to specific B.A.T.M.A.N. forwarding rules. The B.A.T.M.A.N. mesh Network is therefore flooded with Originator messages. This flooding process will be performed by single-hop neighbors in the second step, by two-hop neighbors in the third step, and so forth. OGMs are send and repeated as UDP broadcasts, therefore OGMs are flooded until every node has received it at least once, or until they got lost due to packet loss of communication links, or until their TTL (time to live) value has expired. In practice OGM packet loss caused by interference, collision or congestion is significant. The number of OGMs received from a given Originator via each link-local neighbor is used to estimate the quality of a (single-hop or multi-hop) route. In order to be able to find the best route to a certain Originator, B.A.T.M.A.N counts the originator-messages received and logs which link-local neighbor relayed the message. Using this information B.A.T.M.A.N. maintains a table with the best link-local router towards every Originator on the network. By using a sequence number, embedded in each OGM, B.A.T.M.A.N. can distinguish between new Originator message packets and duplicates ensuring that every OGM gets only counted once.

Destination Sequenced Distance-Vector Routing Protocol (DSDV)

DSDV depends on the periodic exchanging of incremental routing updates or even the entire routing tables among the nodes in the ad hoc network. The periods of advertising these updates should be short enough to adopt with the dynamically changing topology and connectivity conditions of the network. Also, it may allow the exchange of the updates when some significant change in topology or connectivity occurs. Additionally, routing information could be exchanged in response to requests from other nodes.

Optimized Link State Routing (OLSR)

Optimized link state routing is a proactive routing protocol in which each node periodically broadcasts its routing table allowing each node to build a global view of the network topology[5]. The periodic nature of the protocol creates a large amount of overhead. In order to reduce overhead it limits the number of mobile nodes that can forward network wide traffic and for this purpose it uses multi point relays (MPRs) which is responsible for forwarding routing messages and optimization for controlled flooding and operations. Mobile nodes which are selected as MPRs can forward control traffic and reduces the size of control message. Each node independently elects a group of MPRs from its one hop neighbors. MPRs are chosen by a node such that it may reach each two hop neighbor via at least one MPR. The MPRs are responsible for forwarding the control traffic generated by that node. All mobile nodes periodically broadcast a list of its MPR selectors instead of the whole list of neighbors. MPRs advertise link state information for MPR selection periodically in control messages. MPRs are also used to form a route from MN to destination node and perform route calculation. OLSR can forward packets if control traffic received from a previous hop has selected the current node as a MPR. Mobility causes route change and topology changes very frequently and topology control (TC) messages are broadcasted throughout the network. All mobile nodes maintain the routing table that contains routes to all reachable destination nodes. OLSR does not notify the source immediately after detecting a broken link and source node comes to know that route is broken when the intermediate node broadcasts its next packet. OLSR was an was an initial attempt at standardizing a proactive link-state routing protocol.

Clustering/hierarchical routing protocols

A large network can be clustered so that it contains multiple sections or zones[11]. Traffic between clusters is routed by cluster heads. This has as advantage that the routing protocol does not have to deal with all nodes, just the cluster heads. In large networks, super clusters can be made. Every node's hierarchical address is stored in an HSR table and indicates its location in the hierarchy HSR table is updated by the routing update packets Route establishment forward the packet to the highest node in the hierarchy of the source sent to the highest node in the hierarchy of the destination forward from this node to the destination node.

Advantage

Using hierarchy information reduces the routing table size [11].

Disadvantage

The process of exchanging information concerned all the levels of the hierarchy as well as the process of leader election in every cluster makes it quite problematic for ad hoc networks.

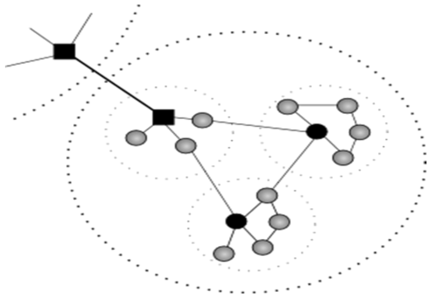

Fig. 4- Clustering routing protocols.

Fisheye State Routing(FSR) protocol

- Uses the fisheye technique to reduce the routing overhead.
- Fish eye has the ability to see objects the better when they are nearer to its focal point.
- That means that: mean each node maintains accurate information about near nodes and not so accurate about far-away nodes.
- Nodes exchange topology information only with their Neighbors.

Basic concept- routing scopes

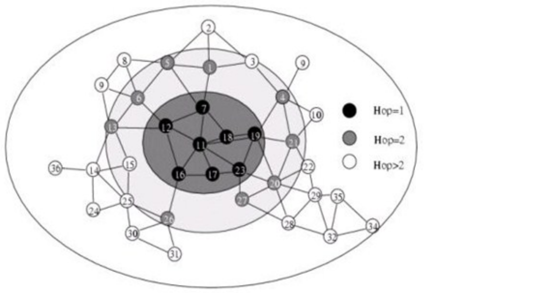

Fig. 5- Fisheye State Routing (FSR) protocol

Another characteristic

Different frequency in exchanging link state information.

- The smaller the scope is the higher the frequency of the exchanges.
- The exchanges in smaller scopes are more frequent than in larger.
- That makes the topology information about near nodes more precise than the information about farther nodes
- However, it results in: less knowledge about distant nodes inaccurate and inadequate information for route Establishing.
- Link break: No control messages after a break

Advantage

- FSR reduces significantly the consumed bandwidth as the link state update packets are exchanged only among neighboring nodes.
- The routing overhead is also reduced due to different frequencies of updates among nodes of different scopes.
- FSR manages to reduce the message size of the topology information due to removal of topology information concerned far-away nodes.

Disadvantage

- Very poor performance in small ad hoc networks.

On-demand routing protocols

The nodes do not exchange any routing information. A source node obtains a path to a specific destination only when it needs to send some data to it. Examples of the protocols of this class are, Dynamic Source Routing protocol (DSR), Ad Hoc On-Demand Distance-Vector Routing protocol (AODV), and Temporally Ordered Routing Protocol (TORA).

Basic Operation of DSR

We base the design of our secure on-demand ad hoc network routing protocol, Ariadne, on the basic operation of the Dynamic Source Routing protocol (DSR)[1]. DSR is an entirely on-demand ad hoc network routing protocol composed of two parts: Route Discovery and Route Maintenance. In this section, we describe the basic form of Route Discovery and Route Maintenance in DSR. In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to find a route; this node is known as the initiator of the Route Discovery, and the destination of the packet is known as the Discovery's target. The initiator transmits a ROUTE REQUEST packet as a local broadcast, specifying the target and a unique identifier from the initiator. Each node receiving the ROUTE REQUEST, if it has recently seen this request identifier from the initiator, discards the REQUEST. Otherwise, it appends its own node address to a list in the REQUEST and rebroadcasts the REQUEST. When the ROUTE REQUEST reaches its target node, the target sends a ROUTE REPLY back to the initiator of the REQUEST, including a copy of the accumulated list of addresses from the REQUEST.

When the REPLY reaches the initiator of the REQUEST, it caches the new route in its Route Cache. Route Maintenance is the mechanism by which a node sending a packet along a specified route to some destination detects if that route has broken, for example because two nodes in it have moved too far apart. DSR is based on source routing: when sending a packet, the originator lists in the header of the packet the complete sequence of nodes through which the packet is to be forwarded. Each node along the route forwards the packet to the next hop indicated in the packet's header, and attempts to conform that the packet was received by that next node; a node may conform this by means of a link-layer acknowledgment, passive acknowledgment, or network-layer acknowledgment. If, after a limited number of local retransmissions of the packet, a node in the route is unable to make this confirmation, it returns a ROUTE ERROR to the original source of the packet, identifying the link from itself to the next node as broken. The sender then removes this broken link from its Route Cache; for subsequent packets to this destination, the sender may use any other route to that destination in its Cache, or it may attempt a new Route Discovery for that target if necessary.

Ad Hoc on Demand Distance Vector (AODV)

Ad hoc on demand distance vector protocol is reactive protocol. It constructs route on demand and aims to reduce routing load[2]. It uses a table driven routing framework, destination sequence numbers for routing packets to destination mobile nodes and has location independent algorithm. It sends messages only when demanded and it has bi-directional route from the source and destination. When it has packets to send from source to destinations mobile node (MN) then it floods the network with route request (RREQ) packets. All mobile nodes that receive the RREQ from neighbor or update message then it checks routing table to find out that if it is the destination node or if it has fresh route to the destination then it unicast route reply (RREP) which is routed back on a temporary reverse route generated by RREQ from source node, or else it re-broadcast RREQ[2].

On-Demand Cache Routing protocol

This protocol presents an efficient algorithm for route discovery, route management and mobility handling for on-demand routing. It is called as "on-demand cache routing" (ODCR) algorithm since it applies caches in each node to improve the routing performance. In the MANET, each node equips L-1 (level 1 or primary) and L-2 (level 2 or secondary) caches. Usually, the size of L-1 cache is about 64 to 256 KB and L-2 cache is about 256 KB to 2MB). For memory address mapping, they use 2-, 4- or 8-way set associative scheme. Each data entry in a cache is called a "cache line". Most caches use the least-recently-used (LRU) policy for cache line replacement. All cache lines can be searched in parallel in a few processor cycles. This is an important reason why many routing protocols adopted cache for route management.

This cache is called as "route cache" because it stores the routing information in the network. For the initial settings of a MANET, this protocol assumes the communication media among nodes (e.g. laptop computers) is RF; each node has an identification (ID) number; each node keeps an ID list in its own cache (see Figure ; the wireless links in the network are symmetric (i.e. bi-directional transmission); and the network is scalable and heterogeneous. This means the number of nodes in the network is changeable anytime, and the processor architecture, transmission radius and battery life of each node can be different. In this section, we only present the main algorithm (ODCR). For detail operations of sub-algorithms RDA and MHA mentioned in Algorithm ODCR below dig space

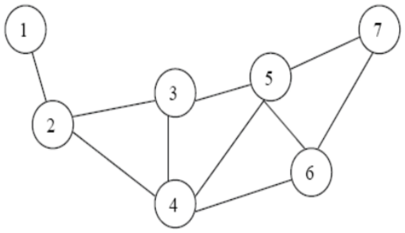

Fig. 6- A simple MANET, where 1, 2, 3, 4, 5, 6 and 7 are node IDs and solid edges are wireless links within the RF transmission radius of each node. For example, node 5 can transmits packets to nodes 3, 4, 6 and 7. In this MANET, each node has an ID list (1, 2, 3, 4, 5, 6 and 7).

Algorithm

On-Demand Cache Routing (ODCR) Inputs: Node identifications (IDs) in the MANET. Outputs: Transmitted data packets on the network.

Begin

- If any node in the network wants to send a data packet, at first it has to search the best route (usually the least hop-count route) from its cache. If the route does not exist, go to Step 2. Otherwise (i.e. the route exists) go to Step 3.
- The source node looks up the destination node in its ID list (as in Figure 6). Then it executes the Route Discovery Algorithm (RDA) to create the best route to its destination node in the network. For instance, the best route from node 1 to node 6 is {1, 2, 4 and 6}.
- The source node attaches its ID, destination node ID and the packet number to each data packet, and sends the packet to the destination node along the best route.
- Each intermediate node uses the best route to the destination node in its cache to forward the data packet to the next or destination node.
- If any node leaves from, joins to, or moves around the network, it has to execute the mobility Handling Algorithm (MHA) to notify other nodes about this change and to update their own route information in their caches.
- Repeat Steps 1 to 5 until the whole network is terminated.

End of On-Demand Cache Routing.

Acknowledgments

We would also like to thank the anonymous referees without support of them it's not possible to improve the Presentation. I earnestly thank my adviser Professor A. D. Raut for his excellent advice and guidance. The immense trust he placed in my abilities was always a great source of motivation

Conclusion

In this research paper, an effort has been made to concentrate on the comparative study and performance analysis of various on demand/reactive routing protocols on the basis of above mentioned performance metrics. It has been further concluded that due to the dynamically changing topology and infrastructure less, decentralized characteristics, is hard to achieve in mobile ad hoc networks. Hence, security and power awareness mechanisms should be built-in features for all sorts of applications based on ad hoc network. The focus of the study is on these issues in our future research work and effort will be made to propose a solution for routing in Ad Hoc networks by tackling these core issues of authentication routing.

We have analyzed that all routing protocol successfully delivers data when subjected to different network stresses and topology changes. Moreover, study results show that DSR protocol, from Reactive

Protocol category, is a very effective, efficient route discovery protocol for Ad-Hoc.

References

[1] Geetha Jayakumar and Gopinath G., *Ad Hoc Mobile Wireless Networks Routing Protocols - A Review*.

[2] Sunil Taneja and Ashwani Kush, *A Survey of Routing Protocols in Mobile Ad Hoc Networks*.

[3] Daniele Furlan, *Analysis of the overhead of B.A.T.M.A.N. routing protocol in regular torus topologies*

[4] Baruch Awerbuch and Amitabh Mishra, *Unicast Routing Protocols for Wireless Ad hoc Networks*.

[5] Nadia Qasim, Fatin Said and Hamid Aghvami, *Mobile Ad Hoc Networking Protocols' Evaluation through Simulation for Quality of Service*.

[6] Amr Ergawy, *Routing Protocols Wireless for Ad Hoc Wireless Networks: Classifications of Protocols and A review of Table Driven Protocols*.

[7] David Murray, Michael Dixon and Terry Koziniec, *An Experimental Comparison of Routing Protocols in Multi Hop Ad Hoc Networks*.

[8] Scott F. Midkiff, *Mobile Ad-hoc Network Routing Protocols: Methodologies and Applications.*

[9] Feeney L., Ahlgren B. and Westerlund A. (2001) *IEEE Communications Magazine,* 39(6).

[10] *Special issue on ad hoc networking*.

[11] Ashwani Kush, Phalguni Gupta and Ram Kumar (2005) *Journal of the CSI*, 35(2).

[12] Kilinkaridis Theofanis, *Hierarchical Routing Protocols*

[13] Sivaram Murthy C. and Manoj B.S. *Wireless Ad hoc Network Architecture & Protocols*.