ISSN 2229-5518

Routing Protocols for Wireless Mesh Networks

Venkat Mohan.S, Dr. Kasiviswanath.N

Abstract— Routing is a fundamental characteristic of Wireless Mesh Network (WMN). The strengths and weakness of routing protocols are reflected directly in WMN's characteristics. Several advantages of WMNs over competing technologies are directly enable by the routing protocols. WMNs require routing protocols that provide flexibility to work with different topologies, low latency for route (re-) discovery, low control traffic overhead, scalability with respect to mobility and network dimension, mobile user support, efficient handover, QoS support, multicast which is important for emergency response cases and more desirable one – multipaths. In this paper, a survey on some of the relevant routing protocols for WMNs, their behavior, and comparison is presented.

Index Terms— AODV, BABEL, B.A.T.M.A.N, Comparison, DSR, FSR, HWMP, OLSR, OFLSR, Protocols, Routing, SHWMP, Wireless Mesh Networks, WMNs.

1 Introduction

WIRELESS Mesh Networks are unstructured networks. Hence routing protocols have to account for mobility, dynamic changes in topology and unreliability of the medium. WMN nodes communicate with each other and they establish routes to non-neighboring nodes. Routing protocols are responsible for discovery, establishing and maintaining such routes. The potential list of route optimization includes the minimum number of hops, interference, delay, error rates, power consumption; the maximum data rates and route stability; use of multiple roots to the same gateway, use of multiple gateways.

The rest of the document is organized as follows. The classification of routing protocols is discussed in Section 2. Section from 3 to 10 discusses about various routing protocols for WMNs followed by the conclusions in Section 11.

2 Classification

Routing protocols for WMNs are mostly based on protocols designed for mobile ad hoc networks. These can be classified in the three categories (Albolhasan, Wysocki and Dutkiewicz – 2004).

2.1 Proactive Routing Protocols

Proactive routing protocols maintain a table for each node representing the entire network topology which is regularly updated in order to maintain the freshness of routing information. At any given time, any node knows how to reach another noe of the network. This approach minimizes the route discovery delay at the cost of exchanging data periodically, which consumes network bandwidth. Proactive protocols are preferred for small networks because of low routing, table lookups. Destination Sequenced Distance Vector (DSDV), Optimized Link State Routing (OLSR), Topology dissemination Based on Reverse-Path Forwarding (TBRPF), Open Shortest Path First – MANET (OSPF-MANET), Fish-eye State Routing (FSR) are some of proactive routing protocols.

2.2 Reactive Routing Protocols

In reactive routing protocols, nodes are not aware of the network topology. Routing table is constructed on-demand. They find routes by flooding network with route requests. This leads to higher latency due to the fact that the route has to be discovered, however it minimizes control traffic overhead. Usually, reactive routing protocols are better suited in networks with low node density and static traffic patterns. Since the traffic patterns are static, the first request encompasses the route discovery, while the subsequent use the previous discovery to route the traffic. On the other hand, proactive protocols are more efficient in dense networks with bursty traffic due to the continous exchange of topology information, reducing route discovery delay. Reactive protocols are preferred for high mobility networks. Dynamic Source Routing (DSR), Ad hoc On-Demand Vector (AODV) and some other extensions derived from AODV are reactive routing protocols.

2.3 Hybrid Routing Protocols

Hybrid routing protocols are mixed design of two approaches mentioned above. The protocols typically use a proactive approach to keep routes to neighborhood nodes (nodes within the vicinity of the source). But for the nodes beyond the vicinity area the protocol behaves like a reactive one. Alternatively, multiple algorithms can be used simultaneously, if WMN is segmented into clusters. Within each cluster a proactive algorithm is used, whereas between clusters a reactive algorithm is used. The challenge is to choose a point, a point from which the protocol should change from practive to reactive.

3 OLSR

[RFC 3626] [2] The Optimized Link State Routing (Jacquet,

- *Venkat Mohan. S, currently pursuing masters degree program in computer science engineering in G.Pulla ReddyEngineering College (Autonomous): Kurnool, Andhra Pradesh, India. E-mail: venkatmohan.s @gmail.com*
- *Dr.N.Kasiviswanath is a professor and Head of CSE Department, G.Pulla Reddy Engineering College (Autonomous): Kurnool, Andhra Pradesh, India.*

Muhlethaler, Clausen, Laouiti, and Qayyum & Viennot 2001) is a practive link state protocol for mobile ad hoc networks. It includes a number of optimizations that aim at reducing the cost of forwarding information in the network. In particular, for each node, a subset of neighbors, called the multipoint relays is to reduce the duplicate retransmissions in the same region.

Algorithm: Each node selects its multipoint relay set among its one-hop neighbors in order to cover all two0hop neighbor nodes. Having a bidirectional link towards each of those neighbors is imposed by OLSR. Each node in the network periodically broadcasts information about its one-hop neighbors which have selected it as a MPR. Upon reception of this MPR selectors list, each node calculates or updates its routes. The route is then a sequence of hops through MPRs. In order to detect bidirectional links with neighbors, each node periodically broadcasts HELLO messages, containing a neighbor list and their link status. HELLO messages contain the list of addresses of the neighbors to whom the node has bidirectional connectivity and the list of neighbors that are heard by the node. The contents of these messages allow each node to know the existence of neighbors up to two-hops and the selection of its MPRs, which are also indicated in the HELLo messages, each node can construct its MPR selector table. Each node broadcasts specific control messages called Topology Control (TC), in order to build the routing table for forwarding purposes. TC messages are sent periodically by nodes to declare its MPR selector set (empty MPR Selector sets are not sent). TC messages are used to maintain topology tables for each node.

Since proactive routing protocol, there is no route discovery delay. Though routing overhead is greater than that of a reactive protocol, it does not increase with the number of routes being used. Default and network routes can be injected into the system. Timeout values and validity information is used.

OLSR assumes that a link is up if a number of hello packets have been received recently. It sees the links either working or failed which is not always true in WMNs.

[3] There are few extensions to link quality features. E.g. OLSRd which is commonly used on Linux based mesh routers have been extended called Radio-Aware OLSR. It has been included in the 802.11s draft standard. It was influenced by Hazy-Sighted Link State (HSLS) protocol.

OLSR unreliably floods the link state DB. So it may cause transient loops if the LS database becomes inconsistent due to packet loss. OLSR propagates data about possibly unused routes. Also OLSR requires sufficient CPU power to compute optimal paths in the network. OLSR causes a lot of routing overhead due to forwarding Topology Control (TC) messages which consumes too much bandwidth resource.

OLSR-NG project, an evolutionary approach tried to address some of the above drawbacks. The original OLSR has O(n*n) where as OLSR-NG has O(n*(log(n)) Dijkstra based.

4 AODV

[RFC 3561/2003] The Ad hoc On Demand Distance Vector (AODV) (Huhtonen 2004) is a reactive protocol that creates and maintains routes only when they are requested. On a given node, the routing table stores only information about the next hop to the desired destination and a sequence number received from the destination, preserving the freshness of the information stored.

Algorithm: AODV message types are: Route REQuests (RREQ), Route REPlies (RREP) and Route ERRors (RERR). On demand, route discovery is done by broadcasting a route request message to the neighbors with the destination and sequence number. Each node that receives the request increases its hop metric and updates its own table. The destination node upon receiving the message, send a route reply back to the requestiong node. Unused entires in the routing table are recycled after a time. When a link fails, a routing error is returned to a transmitting node, and the process repeats.

Nodes respond to link breakages and topology changes in a timely manner. If links break, AODV causes the affected set of nodes to be notified as said earlier a routing error is returned to transmitting node, so that they are able to invalidate the routes using the lost link. AODV is a loop free. By avoiding the Bellman-Ford "counting to infinity" problem, AODV offers quick convergence when the network topology changes (for E.g. Node move).

AODV algorithm enables dynamic, self-starting, multi-hop routing between mobile nodes in an ad-hoc network. Reactive protocols like AODV tends to reduce the control traffic message overhead at the cost of increased latency in finding new routes.

5 OFLSR

Optimized Fish-eye Link State Routing (OFLSR) protocol combines two existing routing protocols: OLSR and Fish-eye State Routing (FSR).

OLSR is discussed above in section 3. FSR belongs to class of proactive (table-driven) ad hoc routing protocols whose mechanisms are based on Link State Routing protocol used in wired networks. It tries to minimize overhead by using a fish-eye technique. It assumes longer link-state update intervals for nodes at higher distances than for network participants in the node]s vicinity. Thus FSR is intended to scale well in large mobile ad hoc networks and supports high rates of mobility.

OLSR causes a lot of routing overhead due to forwarding Topology Control (TC) messages; OFLSR limits this flooding of TC message by adopting fish-eye technique since a source only needs to know approximate route towards the destination far away. [4] With the reduction in link state message sizes, OFLSR performance can be increased.

6 DSR

[RFC 4728/2007] Dynamic Source Routing (DSR) is a simple and efficient routing protocol designed specifically 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 of administration.

DSR uses IP source routing. All the data packets sent that

are sent using DSR protocol contain the complete list of nodes that the packet has to traverse.

Two main mechanisms: route discovery and route maintenance, which work together allows the nodes to discover and maintain routes to arbitrary destinations in the network.

On demand operation – The routing packet overhead of DSR scales automatically to only what is needed to react to changes in the routes currently in use.

The protocol allows finding multiple routes to any destination D. It allows each sender S to select the route based on some criteria such as load balancing and allows controlling the routes used in routing its packets.

It avoids the need for up-to-date route information in intermediate nodes. It reduces the control overhead by eliminating the periodic table-update messages and caching the information learned from other nodes.

The connection setup delay is higher than in table-driven protocols. DSR performs well in static and low-mobility environments, but performance degrades rapidly with increasing mobility. Routing overhead is proportional to the path length due to source routing mechanism employed in DSR.

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

[5] The Better Approach To Mobile Ad hoc Networks (B.A.T.M.A.N) (Johnson, Ntlatalpa, & Aichele 2008) is another proactive protocol for establishing multi-hop routes in mobile ad hoc networks. The development of B.A.T.M.A.N started in [RFC 3626] which was not completely functional in practical scenarios, and particularly for large deployments and in lossy environments. The approach of batman is to spread the knowledge about the best end-to-end paths to all participating nodes. In this approach, each node perceives and maintains information about the only best next hop towards all the other nodes, which avoids unnecessary knowledge about the global topology and reduces the signaling overhead.

Algorithm: Each node *n* broadcasts originator messages (OGM) to inform neighbor nodes about its existence. The neighbors rebroadcast the OGMs to inform their neighbors about the existence of node n, and so on. The network is therefore flooded with these small packets that contain the address of the original node, the address of the node rebroadcasting the packet, a TTL and a sequence number. Each node rebroadcasts the OGM at most once and only if it is received by the current best next hop towards the original initiator of the OGM. Thus OGMs are selectively flooded through the mesh network. Route discovery and neighbor selection depend upon the number and reliability of received OGMs. Sequence numbers are used to perceive the OGM freshness, thus any message received with a lower sequence number than the previous one is dropped. Nodes may alter the TTL of their OGMs to limit the number of hops the message traverses. This is useful for backbone nodes that are deployed only for improved connectivity and coverage purposes.

BATMAN outperforms original OLSR on almost all performance metrics, due to the simplistic approach. By not collecting more information than it can effectively use, and by only getting information about its neighbors, nodes can compute routes in a more efficient manner. Routing overhead is significantly lower than OLSR, providing that sometimes complex approaches lead to less performance.

BATMAN was first released as a classical layer-three (L3) routing protocol, using UDP packets to exchange routing information. Later on, an extension of BATMAN Advanced (batman-adv) was developed to work at layer-two (L2). This version emulates an Ethernet bridge, so that all nodes appear to be attached to a direct link and all protocols operating on the top of it are not aware of the multi-hop nature of the underlying network. The working principles of batman-adv are same as that of classical batman, with adaptions for handling layer-2 (L2) address instead of IP addresses.

8 BABEL

Babel [6] is a proactive advanced distance vector routing protocol. Babel is newer than OLSR and BATMAN. It is designed based on DSDV [7]. The technique of using sequence numbers is borrowed from DSDV in order to prevent count-to-infinity routing loops. Babel also adopts EIGRP's loop avoidance techniques using feasible conditions [8] to quickly converge on loop free paths. Babel uses ETX metric as OLSR does. Babel updates are transmitted unreliably using IPV6. Babel outperforms competing routing protocols in sparse networks.

9 HWMP

[Wang & Lim 2008] IEEE 802.11s adds a third type of network topology called Mesh Basic Service Set or MBSS. An MBSS can have the following three different kinds of entities: a Mesh Station, which is a normal 802.11 Station with added functionality of path discovery and packet forwarding; a Mesh Access Point, which is a Mesh Station that provides client connectivity services and; a Mesh Portal which interconnects the WMN with other non-802.11 networks like 802.3. The 802.11s specifies the Hybrid Wireless Mesh Protocol (HWMP) that runs on the MAC layer, as mandatory for path selection.

Algorithm: Nodes can use two modes of operation, On-Demand Mode and Proactive Tree Building Mode. The On-Demand Mode is based on AODV (Huhtonen 2004), and as stated before, it works at MAC layer. It has three different control packets: Path REQuest (PREQ), Path REPly (PREP) and Path ERRor (PERR). When a node *n* wants to send information, it intitates a PREQ broadcast that floods the network. Every PREQ has a sequence number that allows nodes to perceive its freshness. When an intermediate node receives the PREQ, it either creates or updates the path to the source depending on the sequence number; if there is no path, it simply forwards the request until it reaches the destination. Once the path is established it is cached and subsequent PREQs are not flooded within a small time frame. When the destination node receives the PREQ, it sends a unicast PREP back to node *n*. In the Proactive Tree Building mode of HWMP, one of the nodes acts as ROOT node *r*. The node *r* periodically broadcasts proactive PREQs. The address field of such PREQs is the broadcast address, thus every node that receives them send PREP back to node *r*. In this way, a proactive tree is build, and node *r* has the routing table filled with all possible destina-

tions within the network.

In hybrid mode, both proactive and reactive components act concurrently. Extensibility framework of HWMP allows choosing any routing metric or combinations of metrics. On-demand routing offers great flexibility in changing environments. Proactive tree based routing is very efficient in fixed mesh networks. The combination makes HWMP suitable for implementation on a variety of different network configurations. Default metric is based on airtime. It can be combined with other metrics for better performance.

HWMP protocol elements

1. Root Announcement (Broadcast): tells MPs about the presence and distance of Root-MP (root Mesh Point).
2. Root Request (Broadcast/Unicast): asks the destination MP(s) to form a reverse route to the originator.
3. Route Reply (Unicast): forms a forward route to originator and confirms the reverse route.
4. Route Error (Broadcast): tells receiving MPs that the originator no longer supports certain routes.

On-demand routing in HWMP allows nodes to quickly obtain routes for new destinations. It does not require nodes to maintain routes to destinations that are not in active communication.

Route Discovery: For route discovery, on-demand routing in HWMP uses expanding ring search to limit the flood of routing packets. Reverse paths are set up by Route Request packets (broadcast) from originator and forward paths are set up by Route Reply packet (unicast) send from destination node or intermediate node with a valid route to the destination.

Route Maintenance: Nodes monitor the link status of next hops in active routes. When a link break in an active route is detected, a Route Error message is used to notify other nodes about the loss of link occurred. Route Error message is a broadcast message, hence results in quick notification of route failure.

All the nodes in the network own and maintain a destination sequence number which guarantees the loop-freedom of all routes towards that node.

MPs monitor their upstream links and may switch back up links using RREP; this avoids "re-building" the tree. Loss of upstream link causes RREP to send down. This allows the nodes to decide/select own back-up paths. It signals route holders that same route is broken. In this way tree-based routing maintains the topology.

10 SHWMP

[9] Proposed a Secured Hybrid Wireless Mesh Protocol (SHWMP) as a secure version of HWMP, a secure extension to L2 routing specified in 802.11s. HWMP, in its current form, is vulnerable to various types of routing attacks. SHWMP operates similar to HWMP but uses cryptographic extensions to provide authenticity and integrity of routing messages and prevents unauthorized manipulation of mutable fields in the routing information elements. Though it incurs little computational and storage overhead to ensure security, it is robust against identified attacks and provides higher packet delivery ratio compare to traditional HWMP. [9] Considered the existing key hierarchy of 802.11s hence avoids extra key burden. It identifies the mutable and non-mutable fields in the routing message, protects the non-mutable part using symmetric key encryption and use Merkle-Tree approach to authenticate mutable information. Since it uses only symmetric key operations it is computationally efficient.

11 Conclusion

- Both AODV and OFLSR work very well in Wireless Mesh Networks with small traffic load. As the traffic load increases AODV protocol is not scalable. On the other side, OFLSR provides a better performance in terms of data packet delivery ratio, throughput, packet latency and routing overhead under different traffic and mobility instances [4].
- The current implementation of IEEE 802.11s draft standard provided by open802.11s and batman-adv at layer-2 under static scenarios, batman-adv shows much more reliable performance where open802.11s shows instability. However open802.11s recovers quite rapidly and sometimes even so fsat in case of node failure. On the other hand batman-adv has problems in resuming the communication after an abrupt interuption [10].
- The overhead of OLSR is higher than BATMAN, [11] confirms it. [12] shows larger throughput difference between OLSR and BATMAN whereas [13] suggest that OLSR and BATMAN are similar. Theoritical studies say that BATMAN outperforms OLSR on almost all performance metrics due to simplistic approach as we discussed. Experiments are needed to write a note on this.
- In multihop ad hoc networks, the overhead of routing protocol has the largest impact on throughput. Babel provides higher throughputs in smaller networks. Howeer, it has to be tested in large networks. Testings of [13] provides us the impetus for further experimentation on Babel.
- BATMAN outperforms original OLSR on almost all performance metrics due to its simplistic approach. By not collecting more information than required it can effectively use, and by only getting information about its neighbors, nodes can compute routes in a more efficient manner. Routing overhead is significantly lower than OLSR, proving that some-times complex approaches lead to less overall performance.
- Many research studies [14] confirm that cross layer design system yields higher performance compare to the performance in non-cross layer design systems. HWMP, of its hybrid behavior, is much scalable for Hybrid Wireless Mesh Networks. HWMP with cross layer design outperforms the HWMP with non-cross layer design. HWMP is the default routing protocol for Wireless Mesh Networks.
- SHWMP involves a little calculations of symmetric key encryption yet it outperforms HWMP in non-cross layer system [15]. Though it is confirmed that SHWMP in cross layer design of Wireless Mesh Networks outperforms SHWMP in non-cross layer design WMN theoretically, yet it should be implemented in cross layer design of Wireless Mesh Networks in order to scale in different terms.

REFERENCES

[1] Ian F. Akyildiz and Xudong Wang, "Wireless Mesh Networks" 2009
[2] Thomas Clausen and Philippe Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, October 2003
[3] Christopher Dearlove, ThomasClausen and Philippe Jacquet, "The Optimized Link State Routing Protocol version-2", IETF draft September 2009
[4] Sikander Singh, Sukhwinder Singh, Dr Trilok Anand, "Performance comparison of AODV, OLSR, OFLSR in Wireless Mesh Networks" 2008
[5] Axel Neumann, Corinna Aichele, Marek Linder, "Better Approach To Mobile Ad hoc Networking (B.A.T.M.A.N)", IETF draft, October 2008
[6] Juliusz Chroboczek, "The Babel Routing Protocol", *Internet-Draft*, April 2009
[7] Charles E. Perkins and Pravin Bhagwat, "Highly Dynamic Destination-Sequenced Distance Vector (DSDV) routing for mobile computers", SIGCOMM Computer Communications Review, vol.24, no. 4, pp.234-244, 1994
[8] Bob Albrightson, J.J.Garcia-Luna-Aceves, and Joanne Boyle, "EIGRP-A Fast Routing Protocol Based on Distance Vectors", in Net-World/Interop 94, 1994
[9] George Athanasiou, Thanasis Korakis, Ozgur Ercetin, Leandros Tassiulas, "A Secure Hybrid Wireless Mesh Protocols", in APCC 2009*:* Asia Pacific Conference on Communications, 2009
[10] Rosario G. Garroppo, Stefano Giordano, Luca Tavanti, "Experimental evaluation of two open source solutions for wireless mesh routing at layer-2", 2010
[11] David Johnson, Ntsibane Ntlatlapa, and Corinna Aichel, "Simple pragmatic approach to mesh routing using BATMAN", in 2nd IFIP International Symposium on Wireless Communications and Information Technology in Developing Countries, 2008
[12] Mehran Abolhasan, Brett Hagelstein, and Jerry Wang., "Real-world performance of current proactive multi-hop mesh protocols", in APCC 2009: Asia Pacific Conference on Communications, 2009
[13] David Murray, Michael Dixon, Terry Koziniec, "An experimental comparison of routing protocols in multi-hop ad hoc networks", 2010
[14] George Athanasiou, Thanasis Korakis, Ozgur Ercetin, Leandros Tassiulas, "A cross layer framework for association control in Wireless Mesh Networks", 2009.
[15] Md.Shariful Islam, Md. Abdul Hamid, Choong Seon Hong, "A Secure Hybrid Wireless Mesh Protocol for IEEE802.11s Wireless Mesh Networks", 2009