THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Comparative Analysis of Routing in MANET

Mohammed Farid Zaghloul
Department of Computers and Systems Engineering, Faculty of Engineering, Al-azhar University, Egypt
Reda Hussin Abo El-ezz
Faculty of Engineering, Al-azhar University, Egypt
Mohammed Mahmoud Abo Ghazala
Department of Computers and Systems Engineering, Faculty of Engineering, Al-azhar University, Egypt

Abstract:
Open Shortest Path First (OSPF) is a popular link state routing protocol widely used in Internet infrastructure. OSPF implements several timers to limit the protocol overhead. a link state routing protocol is a popular interior gateway protocol (IGP) in the internet. Modern routing domains need to maintain a very high level of service availability. Hence, OSPF needs to achieve fast conversance to topology changes. Also, the ever-growing size routing domains, and possible presence of wireless mobile ar-hoc components, requires a highly scalable operation on part of OSPF to avoid routing instability. Optimized link– state routing protocol (OLSR) one of the prominent routing protocols for Mobile Ad Hoc Networks (MANET). It is a pro-active protocol where nodes periodically exchanges topology information in order to establish a route to any destination in the network. In this paper we present a comparative analysis between OSPF & OLSR protocol.

Keywords: *OSPF, Fast Convergence, MANET, OLSR.*

1. Introduction

Open Shortest Path First (OSPF) [1] is a successful link state protocol that is widely used in intra-domain ISP networks. In OSPF network, every router establishes adjacency with its connected counterparts and describes the connection status using Link State Advertisement (LSA). Once the topology changes, routers employ specific mechanism, typically Hello protocol prescribed in OSPF standard, to detect the failure and generate new LSAs. After the synchronization of LSAs throughout the network by flooding, routers are capable of calculating the correct routing table for packet forwarding.

Mobile ad hoc network (MANET) is collection of wireless computers (or nodes) establishing a network in which nodes communicate with each other by forwarding packets within and outside range of direct wireless transmission. Such type of networks also known as Mobile Ad Hoc multi-hop wireless networks does not have any requisite for fixed infrastructure or central control such as base station or access point, and can be set up according to the demand anywhere as required [2]. Link state based routing protocols for MANET have been actively developed by the IETF in recent years. The methodology of these protocols can be classified into two broad categories. The first approach is to adapt an existing Interior Gateway Protocol (IGP), such as OSPF, to MANET environments by introducing a new corresponding interface type (e.g., OSPF [3] and OSPF OR [4]). Another approach is to focus more specifically on MANET routing without comprehensive treatment of networking with legacy interfaces supported by de facto standard IGPs.Protocols that fall into this second category include OLSR [5] and TBRPF [6]. Moreover, [7] presents a composite routing approach that allows OSPF to leverage underlying MANET-specific routing. Thus, it can potentially achieve excellent MANET routing performance without losing the main advantage offered by OSPF: routing over existing heterogeneous interface types. However, there are no quantitative results to evaluate the performance of composite routing strategies.

There are a number of possibilities for routing protocols used in layer-3 MANETs. The Internet Engineering Task Force (IETF) has specified a number of experimental MANET routing protocols such as OLSR [8].

These MANET routing protocols have focused on optimizing MANET performance and have not yet been extended to handle more heterogeneous networking environments such as found in larger enterprises. If a MANET is used in a transit networking scenario (i.e., other networks use the MANET as an intermediate network), routing information must be redistributed between the MANET routing protocol and other routing protocols. Redistribution is typically statically configured and may be lossy if one protocol is not capable of fully carrying another's data. The alternative solution for such deployments is to try to reuse an enterprise routing protocol such as Open Shortest Path First (OSPF) [9], [10], but previous experience with OSPF has shown that the protocol does not have suitable mechanisms for operating with high performance over broadcast-based, wireless multihop networks [11]–[13].

In this paper, we investigate the benefits and trade offs among various routing strategies used in Mobile Ad Hoc Networks (MANET). In particular, we compare the performance of OSPF and OLSR. Our composite routing implementation is based on further extensions of OSPF that employs OLSR as the sub-IP MANET routing protocol. The performance evaluation was conducted on an emulation test-bed that utilizes the light-weight Linux network stack virtualization, namely network namespaces. The performance results show that OLSR outperforms OSPF-As a result, composite routing can leverage OLSR to achieve better network performance than OSPF with less overhead.
The remaining paper is structured as follows. In Section 2 we briefly outline how to improve convergence speed and scalability in OSPF & OLSR. Fast failure detection in MANET is given in section 3.Then we present our analysis in detail OLSR rules & steps in Section 4. We also present the OSPF protocol and its components in Section 5, and then describe interconnection between OLSR and OSPF in Section 6. Section 7 discusses security of both. At last we conclude in Section 8.

2. Convergence Speed and Scalability

Faster Failure Detection
Faster and Fewer Adjacency Establishments
Optimizing LSA Generation and Flooding
Optimizing Routing Table Calculations

Table 1: Main steps in improving speed convergence and scalability

Detection of a topology change by the routers in the vicinity.
Convergence speed is one of the important goals that face the wireless protocol. The need for fast convergence and scalability in link-state routers protocols as shown in table 1 continue to challenge the research community as the routing domains grow large and more complex. Convergence to a topology changes can consists of the following steps.

- Adjacency establishment or breakdown by the routers affected by the topology changes.
- The generation pf new LSA by the affected router and their flooding throughout the protocol area.
- Routing table calculation by each router one receiving the LASAs, followed by the distribution of the routing table updates to the line cards. The overall, Convergence delay depends upon the time required to complete each of the steps mentioned above. In this paper we shall focus on these steps and how to reduce delay and improve the Convergence mechanisms.

3. Fast Failure Detection in MANET
How to define the fault in the network and fix it or at least isolate in the shortest time as possible is one of the main methods in order to achieve fast Convergence. There are many ways to speed up the failure detection process starting by hardware based failure detections, Reduced Hello-Interval and including Bidirectional forwarding detection technique. Hardware failures are common in any network and have defined examples such as network failure operations, hardware errors (Such as errors in configuration a protocol) . The failure may manifest itself depends on self-diagnostics parameters in the components in the network .

4. OSPF Protocol on MANET
As a proactive link state, OSPF employs periodic exchanges of control messages to accomplish topology discovery and maintenance: packets
called Hello are exchanged locally between neighbors to establish bi-directional links, while other packets called LSAs reporting the current states of these links are flooded throughout the entire network. This signaling results in a topology map , The link state database (LSDB) , being present in each node in the network , From which a routing table can be constructed . An additional mechanism, particular to OSPF, provide explicit pair-wise synchronization of the LSDB between some neighbors, via additional control signaling (database description messages). Such neighbor pairs are then called adjacent neighbors, while other bidirectional neighbors are called Two-Way. In a wireless ad-hoc environment, there are many problems as limited bandwidth and interference between neighbors call for a significant reduction of OSPF traffic. At the same time, Routers mobility requires Hello and LSA periods to be drastically shortened in order to be able to track topology changes, implying heavier control traffic, without even more efficient control traffic reduction techniques. The standard OSPF mechanism providing control traffic

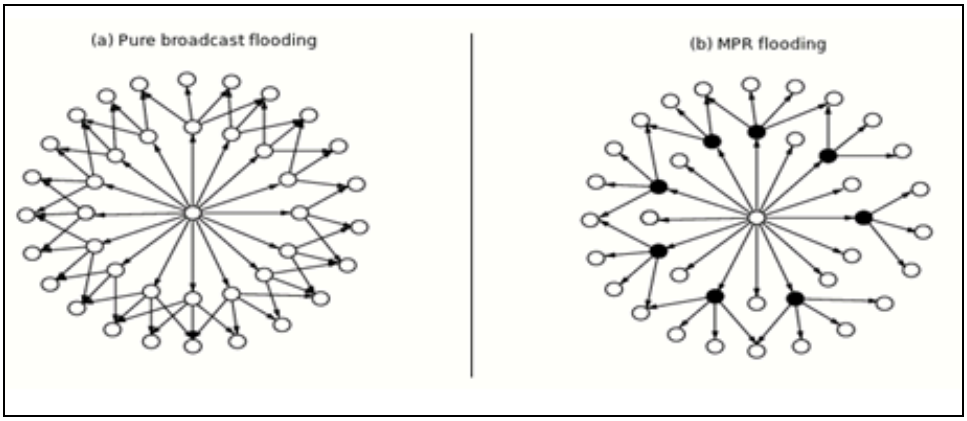

Figure 1: MPR broadcasting vs normal flooding .

reduction the designated router mechanism. However in a wireless ad-hoc environment, this mechanism is not functional due to the fact that wireless neighbors generally do not have the same set of wireless neighbors. OSPF extensions for MANET thus use alternative mechanisms. Aside of miscellaneous tweaks and tricks such as control traffic multi casting (instead of uni-cost). The alternative mechanisms can be classified in the following categories:

- Flood optimization and backup :- Instead of the usual , native flooding scheme , use more sophisticated techniques that reduce redundant retransmission .
- Adjacency selection :- instead of attempting to become adjacent with all its neighbors , A router becomes adjacent with only some selected neighbors .
- Topology Reduction :- Reporting only a partial topology information in LSAs , instead of a full topology information .
- Hellow Redundancy Reduction:- In some hello message , report only changes in neighborhood information instead of full neighborhood information .

5. OLSR Protocol on MANET

OLSR is a proactive protocol where needs periodically exchange topology information in order to establish a route to any destination in the network. The OLSR is an optimization of a pure link-state routing
protocol. Its based on multipoint relays (MPRs). First, using multipoint relays reduces the size of control messages: rather than declaring all its links in the network, a node declares only set of links with neighbors that have selected it s multipoint relay. The use of (MPR) also minimize flooding of control traffic indeed only multipoint relays forward control messages. This techniques significantly reduces the number of retransmission of board cost messages. Each node acquires the knowledge of its one-hop and two-hop neighborhoods by means of periodic Hello messages. it independently selects its own set of multipoint relays cover all its two-hop neighbors. Each node also maintains topological information about the network obtained by means of topology control (TC) messages broadcast by (MPR) nodes the royting table is computed by Dijkstra algorithm . It provides the shortest route (i.e the route with the smallest hop number) to any destinations in the network .

6. Principles of the OSPF/OLSR Interconnection

Interconnections between OLSR and OSPF is a target to all researchers in wireless networks as the OLSR features a simple and efficient mechanism to import routes coming from another routing protocol : host and network association (HNA) messaging with these messages , an OLSR node can advertise it has reach-ability to non-OLSR hosts or networks. For instance, if an OLSR node is also connected via another interface to an OSPF network, it can periodically generate and transmit such HNA messages including the OSPF networks IP-Fixes. Routes to the OSPF network with them be included in OLSR-driven routing tables.
Similarly OSPF features its own mechanism to import routes coming from another routing protocol: link state advertisement (LSA) messages type 5 and 7. These messages advertise routes that are extended to the OSPF network , which are then included in OSPF-driven routing tables , there are however two different types of metrics . In order to achieve OLSR/OSPF interconnection. it's sufficient to use these two mechanisms to transfer routes between OSPF and OLSR through the interface routes (the router that have both OSPF and OLSR interface .

7. Security in MANET

Security topic is on of the most important goals in wireless networks especially in military uses. So the network security has attracted more attention than before but the security concern for routing protocols has not been fully aware by the public. For wireless Ad-Hoc networks, the situation is even-worse. Ad-Hoc networks have no pre-deployed in infrastructure available for routing packets end-to-end ina network. Node communicate with each other without the intervention of centralized access points or base stations, so each node acts as both a router and as a host. Securing Ad-Hoc routing presents difficulties not present in traditional networks: neither centrally administrated secure routers not strict policy exist in an Ad-Hoc network , the nodes in the networks can b highly mobile , thus rapidly changing the node constellation and the presence or absence of link . So, the routing in Ad-Hoc networks in as especially hard task to accomplish securely robustly and efficiently .

7.1. Security of OSPF

OSPF contains two authentication methods. The first one is simple password scheme. The OSPF heads carries a plaintext password so that the routers within the routing domain can share a secret for authentication . It is obvious that is not secure since the password is transmitted in the clear. Another much stronger authentication algorithm is cryptographic message digest, eg keyed MDS with assumption that routers an a common network share a secret key. This is a symmetric crypto-graphic scheme. These are two cases here. If all the routers share the secret key, then the security level is low. If each pairs of routers share a secret key, it requires a O(N2) set of secret keys . So the key distribution process with very complex.

7.2. Security of OLSR

A significant issue on MANET is that of the integrity of the network itself. OLSR allows any node to participate in the network. The assumption being that all nodes are behaving well and welcome. It that
assumption fails, then the networking be subject to malicious nodes and integrity of the network fails. In OLSR as in any other proactive MANET
routing protocol each node must first correctly generate routing protocol control traffic , confirming the protocol specification secondly , each node is reasonable for forwarding routing protocol control traffic in behalf of other nodes in the network. Thus, incorrect behaviors of a node can result from either a node generating incorrect control messages or from incorrect relaying of control traffic from other nodes, Thus, we have two types of attacks against the OLSR routing protocol. The first type of attacks consists, for a node, in generating incorrect control messages. For this type of attacks the node can generate a fake control message from scratch or it can replay already sent control messages. In this second case, we have an incorrect control message generation using replay another even more advanced such replay attack consists in capturing a control message in a a given location of the network and replaying it very rapidly to another location to replay it .

8. Conclusion

In this paper, we presented comparison study results for OSPF, OLSR and composite routing. Composite routing integrates OSPF and OLSR in a novel way such that it solves both MANET routing and IP internetworking without combining the overhead of two protocols. In particular, composite routing eliminates LSA flooding due to topology changes within the MANET (e.g., router LSAs). Furthermore, since a dedicated MANET routing process is in place to handle all MANET-specific routing, the IP routing process can abstract the MANET as a connected mesh and thus reduce the need for flooding topology information through legacy network interfaces. As a result, most mobility is hidden by a more stable topology abstraction of the MANET. We evaluated the performance using lightweight network stack virtualization that enables us to use real implementation code in our experiments. Our measurement results show that OLSR outperforms OSPF. OSPF introduces less overhead when mobility is low. In summary, the composite routing framework is very
attractive for addressing the problem of internetworking legacy IP networks with MANETs.

9. References

1. J. Moy, OSPF version 2, Internet Engineering Task Force, Request For Comments (Standards Track) RFC 2328, April 1998.
2. G. Jayakumar and G. Ganapathy, "Performance Comparison of Mobile Ad-hoc Network Routing Protocol," International Journal of Computer Science and Network Security (IJCSNS), vol.7, No.11, pp. 77-84, Nov. 2007.
3. R. Ogier and P. Spagnolo. Mobile ad hoc network (MANET) extension of OSPF using connected dominating set (CDS) flooding,RFC 5614, August 2009.
4. Roy and M. Chandra. Extensions to OSPF to support mobile ad hoc networking, RFC 5820, Mar. 2010.
5. T. Clausen and P. Jacquet. Optimized link state routing protocol (OLSR),. RFC 3626, Oct. 2003.
6. R. Ogier, F. Templin, and M. Lewis. Topology dissemination based on reverse-path forwarding (TBRPF), RFC 3684, Feb. 2004.
7. J. J. Weinstein, J. R. Zavgren, B. B. Elliott, N. Rehn, and W. S. Passman. Radio networking routing apparatus. United States Patent No. 6,977,937, December 2005.
8. T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626 (Experimental), Oct. 2003.
9. J. Moy, "OSPF Version 2," RFC 2328 (Standard), Apr. 1998.
10. R. Coltun, D. Ferguson, and J. Moy, "OSPF for IPv6," Request for Comments 2740, IETF, December 1999.
11. W. Wollman and Y. Barsoum, "Overview of Open Shortest Path First, Version 2 (OSPFv2) Routing in the Tactical Environment," in Proceedings – IEEE Military Communications Conference MILCOM. Nov. 1995, vol. 3, pp. 925 – 930, IEEE.
12. P. Sass, "Communications Networks for the Force XXI Digitized Battlefield," Mob. Netw. Appl., vol. 4, no. 3, pp. 139–155, 1999.
13. T. Henderson, P. Spagnolo, and J. Kim, "A Wireless Interface Type for OSPF," in Proceedings – IEEE Military Communications Conference MILCOM. Oct. 2003, vol. 2, pp. 1256 – 1261, IEEE.