ISSN 2320-9984

Volume 1, Issue 4, December 2013 ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

A Secure Routing Approach of Optimized Link State Routing Protocol

Deshraj Ahirwar
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email : deshrajahirwar.sati@gmail.com

Abhishek Kesharwani
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email : abhishek040685@gmail.com

Sanjay Kumar Tehariya
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV,
Bhopal (M.P.) [INDIA]
Email : sanjay_tehariya@rediffmail.com

Azher Ahmed Khan
Assistant Professor
Department of Computer Science & Engineering
University Institute of Technology, RGPV
Bhopal (M.P.) [INDIA]
Email : khanazher@yahoo.co.in

***Abstract*—*Since link-state routing requires the topology database to be synchronized across the network, OSPF and IS-IS perform topology flooding using a reliable algorithm. Such an algorithm is very difficult to design for ad hoc wireless networks, so OLSR doesn't bother with reliability; it simply floods topology data often enough to make sure that the database does not remain unsynchronized for extended periods of time.*

Being a proactive protocol, routes to all destinations within the network are known and maintained before use. Having the routes available within the standard routing table can be useful for some systems and network applications as there is no route discovery delay associated with finding a new route.

The routing overhead generated, while generally greater than that of a reactive protocol, does not increase with the number of routes being created.

Default and network routes can be injected into the system by HNA messages allowing for connection to the internet or other networks within the OLSR MANE cloud. Network routes are something reactive protocols do not currently execute well. Timeout values and validity information is contained within the messages conveying information allowing for differing timer values to be used at differing nodes.

***Keywords:*—*MANET, Link state routing, Bandwidth, wi-fi etc.*

1. INTRODUCTION

The **Optimized Link State Routing Protocol** (**OLSR**)[1] is an I routing protocol optimized for mobile ad hoc network, which can also be used on other wireless ad hoc network. OLSR is a proactive link-state routing protocol, which uses *hello* and *topology control* (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.

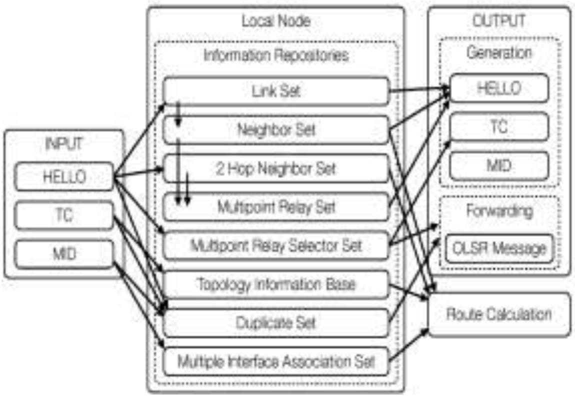

Figure 1: OLSR layered architecture.

Link-state routing protocols such as Open Shortest Path Firs (OSPF) and IS-I elect a designated router on every link to perform flooding of topology information. In wireless ad hoc networks, there is different notion of a link, packets can and do go out the same interface; hence, a different approach is needed in order to optimize the flooding process. Using Hello messages the OLSR protocol at each node discovers 2-hop neighbor information and performs a distributed election of a set of multipoint relay (MPRs). Nodes select MPRs such that there exists a path to each of its 2-hop neighbors via a node selected as an MPR. These MPR nodes then source and forward TC messages that contain the MPR selectors. This functioning of MPRs makes OLSR unique from other link state routing protocols in a few different ways: The forwarding path for TC messages is not shared among all nodes but varies depending on the source, only a subset of nodes source link state information, not all links of a node are advertised but only those that represent MPR selections.

The original definition of OLSR does not include any provisions for sensing of link quality; it simply assumes that a link is up if a number of hello packets have been received recently. This assumes that links are bi-modal (either working or failed), which is not necessarily the case on wireless networks, where links often exhibit intermediate rates of packet loss. Implementations such as the open source OLSRd (commonly used on Linux-based mesh routers) have been extended (as of v. 0.4.8) with link quality sensing.

Being a proactive protocol, OLSR uses power and network resources in order to propagate data about possibly unused routes. While this is not a problem for wired access points, and laptops, it makes OLSR unsuitable for sensor networks that try to sleep most of the time. For small scale wired access points with low CP power, the open source OLSR project showed that large scale mesh networks can run with OLSRd on thousands of nodes with very little CPU power on 200 MH embedded devices.

Being a link-state protocol, OLSR requires a reasonably large amount of bandwidth and CPU power to compute optimal paths in the network. In the typical networks where OLSR is used (which rarely exceed a few hundreds of nodes), this does not appear to be a problem.

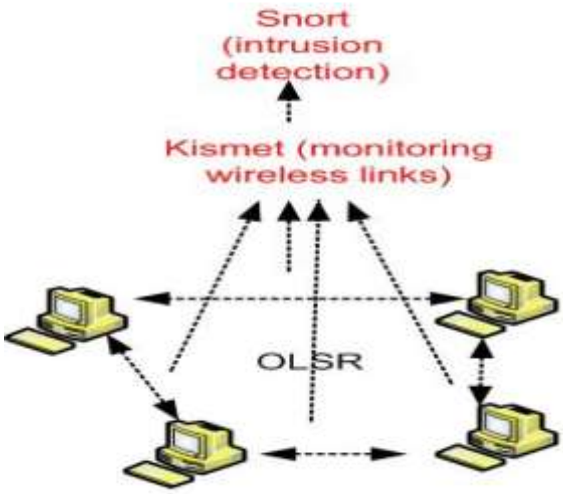
Snort (intrusion detection)
Kismet (monitoring wireless links)
OLSR

Figure 2: OLSR overview in adhoc network

By only using MPRs to flood topology information, OLSR removes some of the redundancy of the flooding process, which may be a problem in networks with moderate to large packet loss rates[2] however the MPR mechanism is self-pruning (which means that in case of packet losses, some nodes that would not have retransmitted a packet, may do so).

2. RELATED WORK

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a route. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Interne.

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network.

The growth of laptop and 802.11/Wi-F wireless networking have made MANETs a popular research topic since the mid-1990s. Many academic papers evaluate protocol and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hop of each other. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

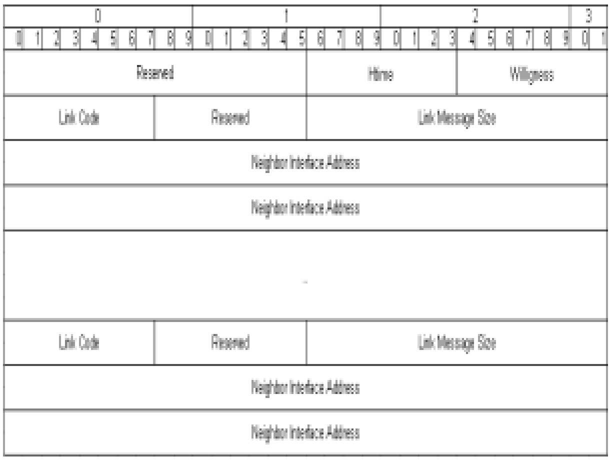

Figure 3: Header format in Routing.

3. LITERATURE REVIEW

Vehicular Ad hoc Network (VANETs) are used for communication among vehicles and between vehicles and roadside equipment

Internet based mobile ad hoc networks (iMANET) are ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. In such type of networks normal adhoc routing algorithms don't apply directly.

Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents, drunken driving etc.

MANETS can be used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications.[2 It should be noted that a key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies.[3 Also researchers have developed performance models[4][5 for MANET by applying Queuing Theory.

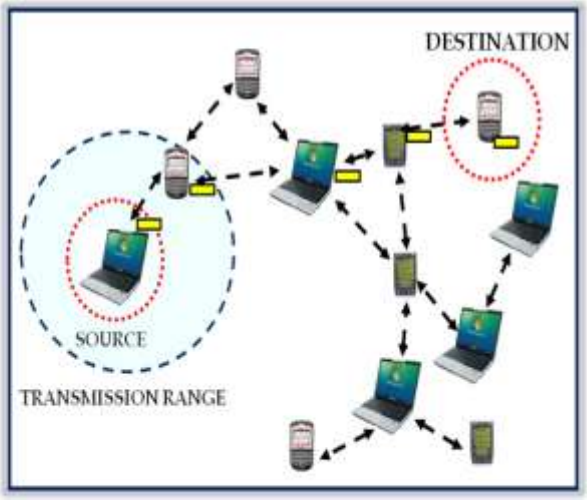

Figure 4: Packet transmission between source and destination

A lot of research has been done in the past but the most significant contributions have been the PGP (Pretty Good Privacy) and trust based security. None of the protocols have made a decent trade off between security and performance. In an attempt to enhance security in MANETs many researchers have suggested and implemented new improvements to the protocols and some of them have suggested new protocols.

Attack classifications

These attacks on MANETs challenge the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a static path of routing. Schematics of various attacks as described by Al-Shakib Khan [1] on individual layer are as under:

- Application Layer: Malicious code, Repudiation
- Transport Layer: Session hijacking, Flooding
- Network Layer: Sybil, Flooding, Black Hole, Grey Hole. Worm Hole, Link Spoofing, Link Withholding, Location disclosure etc.
- Data Link/MAC: Malicious Behavior, Selfish Behavior, Active, Passive, Internal External
- Physical: Interference, Traffic Jamming, Eavesdropping

A VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. Automotive companies like General Motor, Toyot, Nissa, DaimlerChrysle, BM and For promote this term.

Most of the concerns of interest to mobile ad hoc network (MANETs) are of interest in VANETs, but the details differ. Rather than moving at random, vehicles tend to move in an (como dizia o luis costa, a wikipedia nao é fiavel) organized fashion. The interactions with roadside equipment can likewise be characterized fairly accurately. And finally, most vehicles are restricted in their range of motion, for example by being constrained to follow a paved highway.

In addition, in 2006 the term *MANET* mostly described an academic area of research, and the term *VANET* an application.

Such a network might poses safety concerns (for example, one cannot safely type an email while driving). GP and navigation systems might benefit, as they could be integrated with traffic reports to provide the fastest route to work. It was also promoted for free, VoIP services such as GoogleTalk or Skype between employees, lowering telecommunications costs.

4. WORKING

Intelligent vehicular ad-hoc network InVANET) is another term for promoting vehicular networking. InVANET integrates multiple networking technologies such as Wi-F IEEE 802.11, WAVE IEEE 1609, WiMAX IEEE 802.16, Bluetooth, IRA and ZigBee.

Vehicular ad hocal networks are expected to implement wireless technologies such as dedicated short-range communication (DSRC) which is a type of Wi-Fi. Other candidate wireless technologies are cellular, satellite, and WiMAX. Vehicular ad hoc networks can be viewed as component of the intelligent transportation system (ITS).

As promoted in ITS, vehicles communicate with each other via inter-vehicle communication (IVC) as well as with roadside base stations via roadside-to-vehicle communication (RVC).

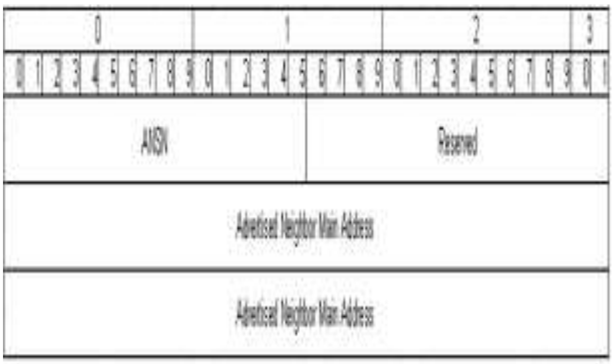

Figure 5: Packet format in adhoc network

5. PROPOSED TECHNIQUE

The problem of routing in ad hoc wireless networks is actively being researched, and OLSR is but one of several proposed solutions. To many, it is not clear whether a whole new protocol is needed, or whether OSP could be extended with support for wireless interfaces.[3][4

In bandwidth-and power-starved environments, it is interesting to keep the network silent when there is no traffic to be routed. Reactive routing protocols do not maintain routes, but build them on demand. As link-state protocols require database synchronization, such protocols typically use the distance vector approach, as in AOD and DSD, or more ad hoc approaches that do not necessarily build optimal paths, such as Dynamic Source Routine.

6. CONCLUSION

OLSRv2 is currently being developed within the IETF. It maintains many of the key features of the original including MPR selection and dissemination. Key differences are the flexibility and modular design using shared components: packet format packetbb, and neighborhood discovery protocol NHDP. These components are being designed to be common among next generation IETF MANET protocols. Differences in the handling of multiple address and interface enabled nodes is also present between OLSR and OLSRv2.

REFERENCES:

[1] **Jump up** M. Abolhasan, B. Hagelstein, J. C.-P. Wang (2009). Real-world performance of current proactive multi-hop mesh protocol.

[2] **Jump up** Extensions to OSPF to Support Mobile Ad Hoc Networking, Madhavi Chandra, Abhay Roy, Mar-10, RFC 582

[3] **Jump up** MANET Extension of OSPF using CDS Flooding, Richard Ogier, Phil Spagnolo, Aug-09, RFC 561

[4] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking. O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[5] Ma, Y.; Richards, M.; Ghanem, M.; Guo, Y.; Hassard, J. (2008). "Air Pollution Monitoring and Mining Based on Sensor Grid in London". Sensors **8** (6): 3601. do:10.3390/s806360. edi

[6] Ma, Y.; Guo, Y.; Tian, X.; Ghanem, M. (2011). "Distributed Clustering-Based Aggregation Algorithm for Spatial Correlated Sensor Networks". IEEE Sensors Journal **11** (3): 641.do:10.1109/JSEN.2010.205691. edi

[7] Kleinrock, Leonard (1975). "Packet Switching in Radio Channels: Part I--Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics.

[8] Shi, Zhefu; Beard, Cory; Mitchell, Ken (2008). "Tunable traffic control for multihop CSMA networks.

[9] "A Comparative study of MANET and VANET Environment. Journal of Computing **2** (7). 7 2010. Retrieved 28 October 2013.