An Experimental Study on Optimized Link State Routing Protocol for Underground Mines

C.Jeyalakshmi, Assistant Professor, Department of CSE, SIT, Dr.R.Sukumar, Professor, Department of CSE, SIT

***Abstract* —In this paper, we investigate the benefits of Optimized Link State Routing Protocol used for communication in underground mines. Due to network failures, node and link failures in the past few years an explosive growth in the use of wireless routing protocols for communication needs in the underground environment. Most studies indicate that it is impossible for reliable routing under ground level. In this paper, we compare the analysis of the OLSR (Optimized Link State Routing) Protocol and OSPF (Open Shortest Path First) protocol. The performance results shows that OLSR protocol work efficiently since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. Furthermore, OLSR routing can significantly reduce overheads caused by link-state flooding using two techniques MPRs (Multipoint Relays) and Link-state Reduction.**

***Index Terms* — routing, underground, OLSR, OSPF, Performance analysis, multi-hop, flooding, optimization, link-state, Multi Point Relays.**

I. INTRODUCTION

Research on underground communication technologies in mines has been on going since 2006, the mining industry had inherent problems that limited communication capabilities. At present, in most underground mines, people acquire the information by wired communication network, which bring on many problems. Because of the narrowness of the mine, the maintenance of the communication lines becomes harder. If the communication lines break, the whole monitoring system may be destroyed. But the invention of the WSN (Wireless sensor network) proposes a new method to settle these problems. WSN, which integrates sensor technology, embedded computing, distributed information system and wireless communication technology.

Routing protocol is one of the most important components of WSN. Routing protocol has to monitor the change of network's topological structure, exchange the routing information, locate the destination node, choose the route and transfer information through the route. The routing protocols are classified into Proactive and Reactive protocol.

Proactive protocols are based on periodical link-state updates using control packets and therefore generate extra traffic that weigh down the actual data traffic. It maintains extensive routing tables for the entire network. As a result, a route is found as soon as it is requested. The main advantage of a proactive protocol is its low latency in discovering new routes. However, proactive protocols generate a high volume of control messages required for updating local routing tables. OLSR and OSPF are examples of proactive protocols. Contrary to proactive algorithms, reactive protocols tries to find a route from S to D only on-demand, i.e., when the route is required. A Reactive protocol avoids the prohibitive cost of routing information but do not guarantee creation of optimal routing tables. While the idea results in good average performance, the worst-case latency could be high in discovering routes. An example of reactive protocol is the Ad-hoc On Demand Distance Vector (AODV) and Distance DSR (Dynamic Source Routing).

A major goal of this paper is to increase the coverage area and to improve the communication level under the mine. In this paper, we formally analyze the performance of the OLSR and contrast it with that of OSPF. This paper discusses the results of data packet size vs. throughput, data packet size vs. lost, data packet size vs. jitter and bandwidth vs. throughput. In this paper, we evaluate the performance of both OLSR and OSPF approaches the simulation results validate the performance evaluation and shows that OLSR provides better stability and availability than OSPF under the mining areas.

II. OVERVIEW OF OLSR

To give more prospective about the performance of the routing protocols, this section discusses about the OLSR. Because of the inefficiency of the OSPF protocol the OLSR protocol was invented. OLSR protocol is a link state protocol such as OSPF, but it optimizes the control overhead in the network. In wireless environments, OSPF's routing causes wasted overhead that often saturates the wireless medium with control traffic for routes that are never used. OSPF needs relevantly much time to converge, as messages are transmitted from one node to another. This may introduce instability, particularly when nodes are also moving.

The OLSR is a table-driven pro-active protocol. As the name suggests, it uses the link-state scheme in an optimized manner to diffuse topology information throughout the network. OLSR uses this approach as well, but since the protocol runs in wireless multi-hop scenarios the message flooding in OLSR is optimized to preserve bandwidth. Being a table-driven protocol, OLSR operation mainly consists of updating and maintaining information in a variety of tables. The data in these tables is based on received control traffic, and control traffic is generated based on information retrieved from these tables. It is important to understand that OLSR does not route traffic. It is not in any way responsible for the actual process of routing traffic. OLSR could rather be described as a route maintenance protocol in that it is responsible for maintaining the routing table used for routing packages, but such protocols are usually referred to as routing protocols.

The route calculation itself is also driven by the tables. OLSR defines three basic types of control messages,

HELLO - HELLO messages are transmitted to all neighbors. These messages are used for neighbor sensing and MPR calculation.

TC - Topology Control messages are the link state signaling done by OLSR. This messaging is optimized in several ways using MPRs.

MID - Multiple Interface Declaration messages are transmitted by nodes running OLSR on more than one interface. These messages list all IP addresses used by a node.

As a derivate of the classical link-state algorithm, OLSR maintains state by keeping a variety of databases of information. These information repositories are updated upon processing received control messages and the information stored is used when generating such messages. Here follows a brief look at the different information repositories used in core OLSR.

Multiple Interface Association Information Base

This dataset contains information about nodes using more than one communication interface. All interface addresses of such nodes are stored here.

Link Set

This repository is maintained to calculate the state of links to neighbors. This is the only database that operates on non-main-addresses as it works on specific interface-to-interface links.

Neighbor Set

All registered one-hop neighbors are recorded here. The data is dynamically updated based on information in the link set. Both symmetric and asymmetric neighbors are registered.

2-hop Neighbor Set

All nodes, not including the local node, that can be reached via a one-hop neighbor is registered here. Notice that the two hop neighbor set can contain nodes registered in the neighbor set as well.

MPR Set

All MPR's selected by the local node is registered in this repository. The MPR concept is explained in section IV.

MPR Selector Set

All neighbors that have selected this node as a MPR are recorded in this repository.

Topology Information Base

This repository contains information of all link-state information received from nodes in the OLSR routing domain.

Duplicate set

This database contains information about recently processed and forwarded messages.

These repositories are needed in order to support reliable routing and communication mechanism. Since it is not easy to implement a large network for experimental purposes under the mining, we perform a simulation to analyze the performance of routing OLSR for limited nodes.

III. OLSR FUNCTIONALITY

In OSPF routing if the message is transmitted from one node to another it needs relevantly much time to converge and also introduce instability, particularly when nodes are also moving. Because of the inefficiency of the OSPF protocol, the OLSR protocol was invented. The packet format of OLSR is shown below,

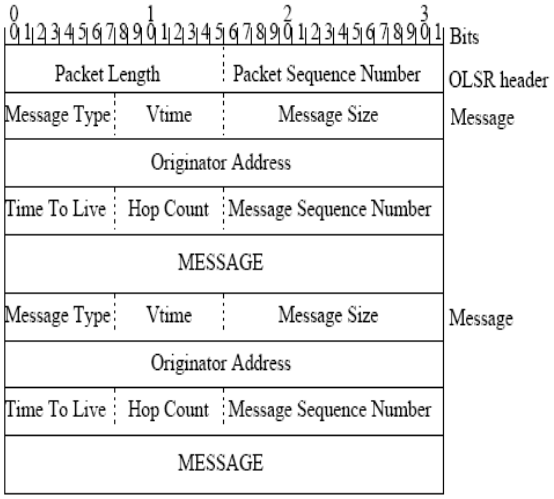

Fig. 1. The OLSR packet format.

The fields in the OLSR packet header are:

Packet Length -Size of the packet in bytes.

Packet Sequence Number - A sequence number incremented by one each time a new OLSR message is transmitted by this host. A separate Packet Sequence Number is maintained for each interface so that packets transmitted over an interface are sequentially enumerated. An OLSR packet body consists of one or more OLSR messages. OLSR messages use a header as shown in fig.1. All OLSR messages must respect this header. The fields in the header are:

Message type - An integer identifying the type of this message. Message types of 0-127 are reserved by OLSR while the 128-255 space is considered "private" and can be used for custom extensions of the protocol.

Vtime - This field indicates for how long after reception a node will consider the information contained n the message as valid. The time interval is represented in a mantissa-exponent format.

Message Size - The size of this message, including message header, counted in bytes.

Originator Address - Contains the main address of the node which originally generated this message. This field should not be confused with the source address from the IP header, which is changed each time to the address of the intermediate interface which is retransmitting this message. The Originator Address field must never be changed in retransmissions.

Time To Live - The maximum number of hops this message can be forwarded. Using this field one can control the radius of flooding.

Hop Count - The number of times the message has been forwarded.

Message Sequence Number - A sequence number incremented by one each time a new OLSR packet is transmitted by this host.

OLSR optimizes the control overhead in the network via two methods:

1. Multi point Relay
2. Link-state reduction

IV. MULTIPOINT RELAYING

The key concept used in the protocol is that of multipoint relays. MPRs are selected nodes which forward broadcast messages during the flooding process. This technique substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message. In OLSR, link state information is generated only by nodes elected as MPRs. Thus, a second optimization is achieved by minimizing the number of control messages flooded in the network. As a third optimization, an MPR node may chose to report only links between itself and its MPR selectors. Hence, as contrary to the classic link state algorithm, partial link state information is distributed in the network. This information is then used for route calculation. OLSR provides optimal routes (in terms of number of hops). This protocol is particularly suitable for large and dense networks and the concept of multipoint relaying is to reduce the number of duplicate retransmissions while forwarding a broadcast packet.

This technique restricts the set of nodes retransmitting a packet from all nodes, to a subset of all nodes. The scenario illustrated in fig. 2, node A selects the black nodes as MPRs. This way all two hop nodes can be reached through a

MPR. Node B will not retransmit traffic from A that is to be flooded.

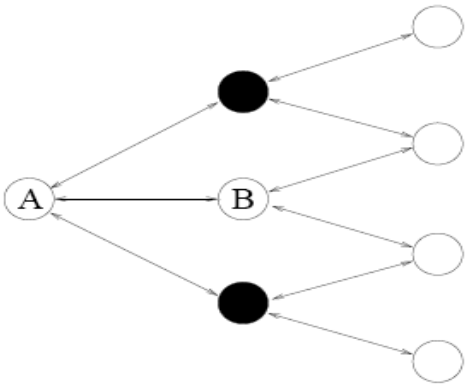

Fig. 2. Node A has selected the black nodes are its MPRs

The OLSR nodes lets announce their willingness to act as MPRs for neighbors. 8 levels of willingness are defined from the lowest WILL_NEVER (0) which indicates that this node must never be chosen as a MPR, to the highest WILL_ALWAYS (7), which indicates that this node should always be chosen as a MPR. The willingness is spread through HELLO messages and this information must be considered when calculating MPRs.

V. FORWARDING OLSR ROUTING ALGORITHM

OLSR specifies a default forwarding algorithm that uses the MPR information to flood packets. One is however free to make ones own rules for custom forwarding of custom messages. But all messages received that carries a type not known by the local node, must be forwarded according to the default forwarding algorithm. The algorithm can be outlined as:

1. If the link on which the message arrived is not considered symmetric, the message is silently discarded. To check the link status the link set is queried.
2. If the TTL carried in the message header is 0, the message is silently discarded.
3. If this message has already been forwarded the message is discarded. To check for already forwarded messages the duplicate set is queried.
4. If the last hop sender of the message, not necessarily the originator, has chosen this node as a MPR, then the message is forwarded. If not, the message is discarded. To check this, the MPR selector set is queried.
5. If the message is to be forwarded, the TTL of the message is reduced by one and the hop-count of the message is increased by one before broadcasting the message on all interfaces.

Link set optimization

Due to the nature of the MPR selection, only nodes which are chosen as MPRs by one or more neighbors, needs to declare their link-state. In fact, these nodes need only declare the MPR selectors in the linkstate messages. When this information is flooded to all nodes in the MANET, all nodes will have enough information to calculate shortest path routes to all hosts.

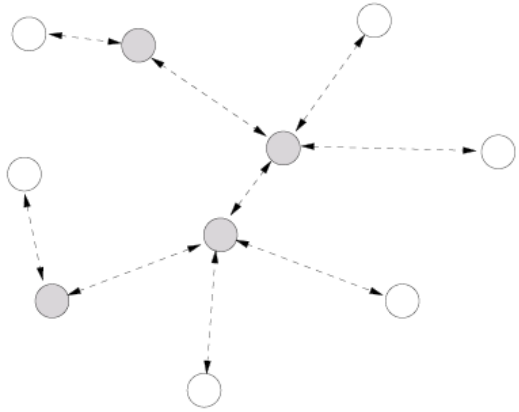

Fig.3. Gray nodes are chosen as MPRs by 1or more neighbors in an OLSR Routed Network

The default OLSR setting is that a node only floods link-state messages if it is chosen as MPR by at least one neighbor, and it only announces its MPR selectors in these messages. In the topology illustrated in the figure 3. Only the nodes selected as MPRs(gray nodes) by one or more neighbors will transmit link-state messages. One can easily see that this information, in addition to some neighbor-sensing scheme, will be sufficient to create a full understanding of the topology. Using the Multiple Interfaces nodes participating in an OLSR routing domain can be multi-homed. That means that they can run OLSR on multiple communication interfaces using multiple identifiers. Multiple interface declaration (MID) messages is used to diffuse information about multi-homed nodes. A MID message is essentially just a list of addresses used by interfaces on which a node runs OLSR. The data is sent as the

message part of an OLSR-message included in an OLSR packet as seen in figure1.

After receiving a MID message, a node updates is Multiple Interface Association Information Base according to the information carried in the message. All OLSR interfaces listed in the MID message are registered on the main address of the originator. The main address is found in the originator field of the OLSR-message header. When adding a route to a node, OLSR will add routes to all addresses of other interfaces on which the remote node runs OLSR, using the same path. All nodes running OLSR on more than one interface are generating MID messages on regular intervals. MID messages are to be flooded throughout the network using the default forwarding algorithm.

Neighbor discovery

In OLSR it needs some mechanism to detect neighbors and the state of the communication lines to them. HELLO messages are emitted on a regular interval for this purpose.

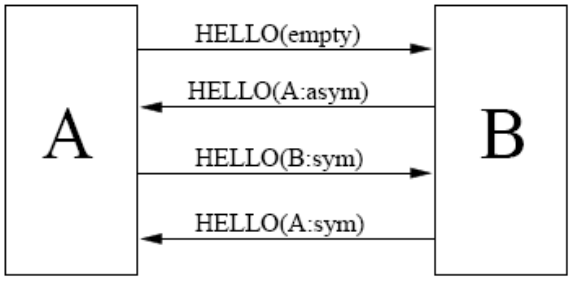

Fig.4. A typical neighbor discovery session using HELLO messages.

The simplified version of a neighbor discovery session using HELLO messages is displayed in figure 4. A first sends an empty HELLO message B receives this message and registers A as an asymmetric neighbor due to the fact that B can not find its own address in the HELLO message. B then sends a HELLO declaring A as an asymmetric neighbor. When A receives this message it finds its own address in it and therefore sets B as a symmetric neighbor. This time A includes in the HELLO it sends, and B registers A as a symmetric neighbor upon reception of the HELLO message. But a HELLO message serves other purposes as well. They are generated and transmitted to all one-hop neighbors to achieve link-sensing, neighbor-sensing, two-hop neighbor-sensing and MPR selector sensing.

Link Sensing

To keep up-to-date information on what links exist between a node and its neighbors, the link set is maintained. In HELLO messages a node emits all information about the links to neighbors from the interface on which the HELLO is transmitted. When declaring the neighbor state of neighbors not reachable on the interface on which the HELLO is transmitted, the main address of the neighbor node is used.

VI. EXPERIMENTAL RESULTS

All experiments reported in this section were performed on a Pentium-IV 2.7 GHz machine with 250GB of main memory, running linux (Ubuntu) operating system. The simulation is carried out in NS2 using Tcl/Tk language. Ns are an object oriented simulator, written in C++, with an OTcl interpreter as a front-end. Figure 5 shows just the creation of few nodes and assigning a source node as node 4 in the OLSR routing system.

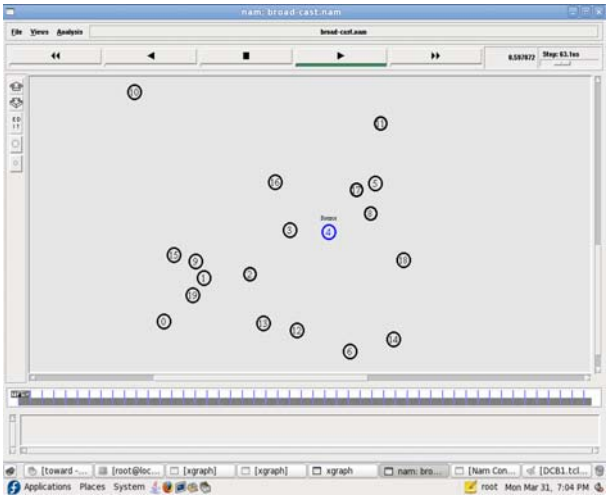

Fig. 5. Creation of some nodes

When source node 4 wants to broadcast packets then it selects MPRs. This way all two hop nodes can be reached through a MPR. Only the nodes selected as MPRs (Rose colored nodes in the figure.6) by one or more neighbors will transmit link-state messages within the transmission range When the node's mobility increases, the delivery ratio drops significantly. The reason for this is that the high mobility of nodes makes node neighbour sets outdated quickly. This incorrect neighbour set

information may lead to more nodes missing the broadcast packet.

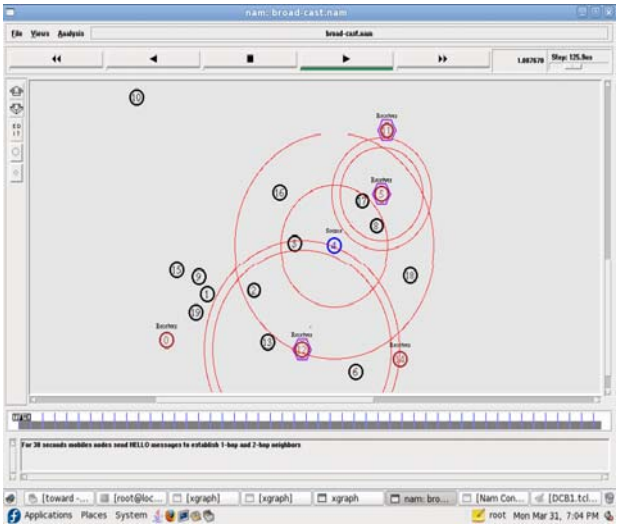

Fig. 6. Selection of MPRs nodes

In OLSR routing the Neighbor detection populates the 1-hop neighbor repository and only uses the main addresses of nodes. As seen in the figure 7, the neighbor entries are closely related to the link entries. Whenever a link entry is created, the neighbor table is queried for a corresponding neighbor entry. Note that this neighbor entry must be registered on the main address of the node. If no such entry can be located, then a new neighbor entry is created. This means that while a node can have several link-entries describing different links to the same neighbor, only one neighbor entry exists per neighbor.

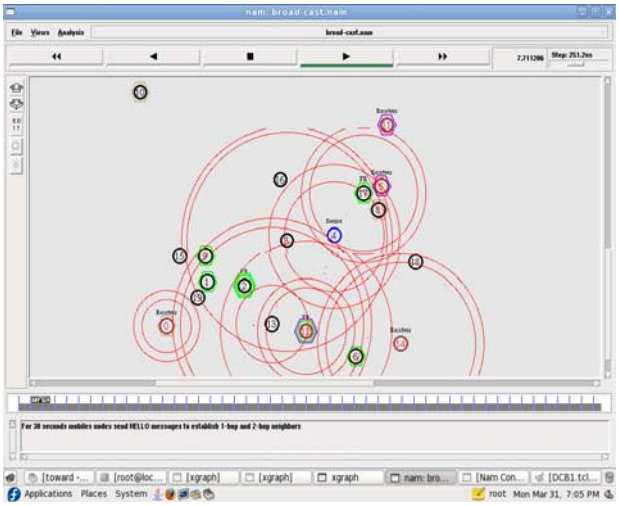

Fig. 7. Increasing of Mobility

The graphs showed below examined the results of data packet size vs. throughput, data packet size vs. lost, data packet size vs. jitter and bandwidth vs. throughput using OLSR.

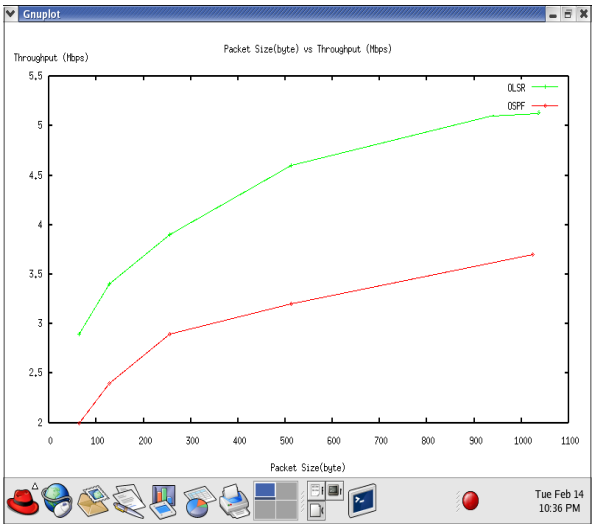

Fig.8. Packet Size Vs Throughput

In the figure 8 we compare the Packet size Vs Throughput of both OLSR and OSPF system. When the packet size is increases the throughput does not affect it also increased.

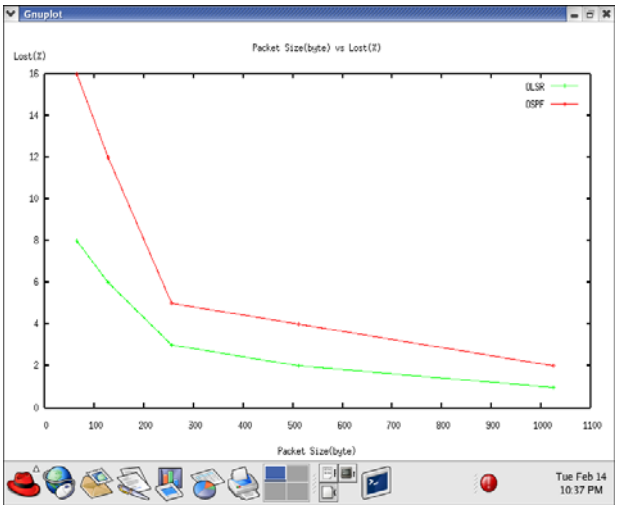

Fig.9. Packet size Vs loss of packet

In the figure 9 we compare the Packet size Vs loss of packet for both OLSR and OSPF system. When the packet size sent are increased in OLSR the losing of packet level is decreased when compare to OSPF.

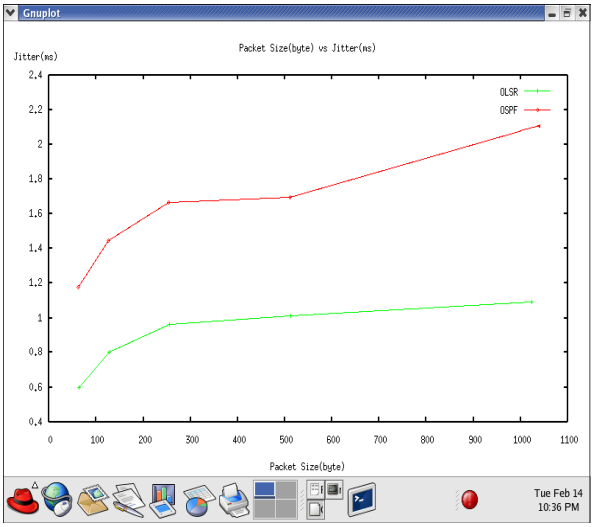

Fig.9. Packet size Vs Jitter

In the figure 9 we compare the Packet size Vs Jitter for both OLSR and OSPF system. When the packet size are increased in OLSR the jitter noise level is minimum when compare to OSPF.

VII. CONCLUSIONS

In this paper, we presented the OLSR functionality for small networks and contrast OLSR with that of OSPF routing. In particular, OLSR routing eliminates flooding due to topology changes within the network. Furthermore, since a dedicated routing process it provides better packet delivery than OSPF. The future work on this functionality will be optimization and bug fixing. This includes dynamic addition and removal of interfaces to use and declaration of multiple IPv6 addresses belonging to the same interface, in MID messages. The link layer functionality is the only unfinished part of the OLSR implementation also; there is a problem of the maximum limit of MAC addresses one can register with the drivers. To overcome this, a simple recompilation of the drivers with a higher max-value, can be enough. A solution could be a scheme where neighbors selected as MPRs are prioritized if the maximum limit is reached when registering neighbors with the driver. This information could be injected into the ARP cache directly. Such a solution would also eliminate the ARP lookups when nodes initiate regular traffic to neighbors.

REFERENCES

[1] A. Roy and M. Chandra. Extensions to OSPF to support mobile ad hoc networking, March 2010. RFC 5820.

[2] Chen Wenqi, Xu Zhao (2010)-“Multi-hop Routing for Wireless Network in Underground Mines,”2010 Asia-Pacific Conference on Wearable Computing Systems,pp.337-340,2010.

[3] S. Mirtorabi, A. Roy, B. E. Weis, and R. Fluhrer. Method and apparatus to minimize database exchange in OSPF by using a SHA-1 digest value. United States Patent No. 7,664,789, Feburary 2010.

[4] Gangzhu QIAO, Jianchao ZENG, (2010)-“An Underground Mobile Wireless Sensor Network Routing Protocol for Coal Mine Environment,” Journal of Computational Information Systems,pp. 2487-2495,2010.

[5] R. Ogier. Comparison of OSPF-MDR and OSPF-MPR, March 2010. draft-ogier-ospf-manet-mdr-mpr-comparison-03.txt.

[6] Zhi Sun, Ian F.Akyildiz (2010)-“Channel Modeling and Analysis for Wireless Networks in Underground Mines And Road Tunnels,” IEEE Transactions on Communication,pp. 1758- 1768 ,Vol 58,2010.

[7] Z. Zhang, X. Xu, L.Yan (2009)- "Underground localization algorithm of wireless sensor network based on Zigbee," Journal of China Coal Society,2009.

[8] WANG Wen-xing, ZHANG Jin-hua, “Design and Implementation of Communication Based on Multi- carrier modulation in mine,” IEEE on Water Resources and Electric Power,2008.

[9] C. O. Hargrave, J. C. Ralston and D. W. Hainsworth (2009)- “Optimizing Wireless LAN for Long wall Coal Mine Automation," Industry Applications, IEEE Transactions,vol.43,pp. 111-117,2009.

[10] L. Yu, A. Li, Z. Sun, and H. Li (2008)- Design of Monitoring System for Coal Mine Safety Based on Wireless Sensor Network," in Mechtronic and Embedded Systems and Applications.MESA 2008. IEEE/ASME International Conference, pp. 409- 414,2008.

[11] P. A. Spagnolo and T. R. Henderson. Connecting OSPF manet to larger networks. In *Proceedings of Milcom 2007*, October 2007

[12] P. A. Spagnolo and T. R. Henderson. Comparison of proposed OSPF manet extensions. In *Proceedings of Milcom 2006*, October 2006.

[13] H. Aniss, et al, - "Communications network for underground mines based on the IEEE 802.11 and DOCSIS standards" in Vehicular Technology Conference,2004 IEEE 60th,pp.3605-3609, Vol. 5

[14] R. Ogier, et al, "Topology Broadcast Based on Reverse-Path Forwarding (TBRPF)", draft-ietf-manettbrpf- 05.txt, March 1, 2002.

[15] D. Johnson, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", draft-ietf-manetdsr- 07.txt, Feb. 21, 2002.

[16] C. Santivanez and R. Ramanathan, "Hazy Sighted Link State Routing: A Scaleable Link State Algorithm", BBN Tech. Memo #1301, Aug. 31, 2001.

[17] C. Perkins, et al, "Ad hoc On-Demand Distance Vector (AODV) Routing", draft-ietf-manet-aodv-10.txt,Jan. 19, 2002.

[18] Z. Haas and M. Pearlman, "Determining the Optimal Configuration for the Zone Routing Protocol", IEEE JSAC, Special Issue on Ad-Hoc Networks, August 1999.

[19] T. Clausen, et al, "Optimized Link State Routing Protocol", draft-ietf-manet-olsr-06.txt, Sep.1, 2001. (www.ietf.org/html.charters/manet-charter.html for the latest versions of these Internet Drafts or subsequent RFCs.)

Jeyalakshmi is an Assistant Professor of Computer Science and Engineering in Sethu Institute of Technology, Virudhunagar. She received her B.Tech degree in Information and Technology from Anna University, Tamilnadu, India, in 2005. She has received her M.E degree in Computer Science and Engineering from Anna University, Tamilnadu, India, in 2007. She is currently pursuing her PhD. degree. Her research interests include Routing and Wireless Network Communication.

Sukumar is a Professor of Computer Science and Engineering in Sethu Institute of Technology, Virudhunagar. He received his B.E Degree in Electronics and Communication Engineering from Madurai Kamaraj University, Tamilnadu, India, in 1992. He has received M.E degree in Computer Science and Engineering from Manonmaniam Sundaranar University, Tirunelveli, Tamilnadu, India,in 2005. He has received his Ph.D Degree from Anna University chennai,Tamilnadu, India, in 2010. His research interests include cryptography and Network Security and he has published 5 papers in reputed international journals.