International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-3, February 2013

Optimize OLSR with Cognitive in Wireless Mesh Network

Manpreet Kaur, Kunwarpal

ABSTRACT- In this paper, we review the COLSR; Cognitive Optimized Link State Routing in Wireless Mesh Network. COLSR is the extension of OLSR Protocol. With the use of COLSR the throughput and performance are enhanced. COLSR provide better solution to the problem of congestion on the nodes, with surely data are transmitted. In this paper, we also discuss the enhancement of OLSR which is purely different from existing OLSR, and also discuss the generation, reputed-trust mechanism along with weighting mechanism from the nodes and COLSR perform re-routing for degrade the packet dropping problem and enhance throughput devoid of congestion on nodes in WMN.

Index Terms-Congestion,WMN, Routing protocol.

I. INTRODUCTION

A Wireless Mesh Network is a special type of wireless ad hoc network. A WMN is implemented to provide dynamic and cost effective connectivity over a specified geographical area. WMN have three main components are: gateways, mesh clients and routers.

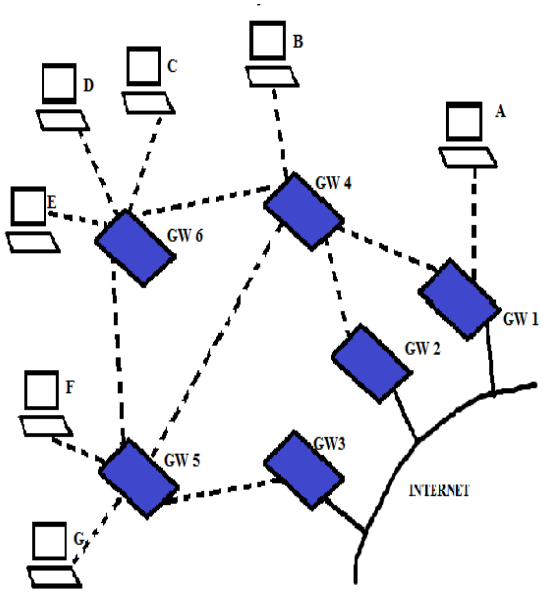

Fig1: Wireless Mesh Network.

Manuscript published on 30 February 2013.
* Correspondence Author (s)
Manpreet Kaur, Research Scholar, Done M.Sc(CS) from GNDU, Amritsar, now doing M.Tech (CSE) from Lovely Professional University, Phagwara, Punjab, India.
Kunwarpal, Assistant Professor in Department of Computer Science, Lovely Professional University, Phagwara, Punjab, India.

The mesh clients are laptops, mobiles and other wireless devices, the mesh routers forward traffic to and from the gateways [14].A mesh network are reliable and redundant. When one of the nodes is damaged the other nodes can still communicate with each other. The node is interacting with each other directly or indirectly. The Wireless Mesh Networks used cognitive should also ensure that the data takes most suitable path from source to destination with same hop count. When two nodes interact indirectly, intermediate nodes between two nodes cooperate each other and are responsible for data forwarding. To establish efficient direct and indirect communication link between the independent nodes of wireless mesh network a trust relationship must be maintained between the nodes in wireless mesh network. An efficient mechanism to maintain trust relationship of the nodes and give the weight _age according to the trust level of the nodes. Before communicating to the other nodes in the network every node must be trusted. When nodes are trusted many type of attacks like replay attack are prevented.

Cognitive Optimized Link State Routing Protocol:

COLSR protocol is the modified version of OLSR. OLSR is based on the proactive (table driven) routing protocol, so the route are available when it needed. The need of OLSR routing protocol to gain more reliability and efficiency. During the wireless, the WMN has some shortcoming while transmission the data between the nodes because some nodes have misbehaving either intentionally or unintentionally. In the OLSR the each node broadcast the link state information to all the other nodes .OLSR uses the HELLO messages for link state information. The MPR (Multipoint Relay) is the key idea behind the OLSR to reduce the information exchange overhead. An MPR reduces the number of the host which multicast the information throughout the network. All other nodes do not multicast route packets.

When source node broadcast the message all its neighbours are receive message. Only the MPR which have not seen the message before again propagates the messages. The flooding overhead is reduced.

We are discussing three types of OLSR control messages:-

HELLO: HELLO messages are transmitted to all the neighbours. These messages are used for finding the information about the link status and the host's neighbours and MPR calculation.

TC: Topology Control messages are the link state signalling done by OLSR. These messages are broadcast throughout the network.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

These messages are used for broadcast information about own advertised neighbour which include at least the MPR selector list. The TC messages are propagate periodically and only the MPR hosts can forward the TC messages.

MID: Multiple Interface Declaration messages are transmitted by nodes running OLSR on more than one interface. These messages list all AP addresses used by a node. The MID messages are broadcasted throughout the entire network only by multipoint relays.

The OLSR is one of the most popular proactive routing protocols because it broadcast its link state information rather than routing tables. Due to this feature it's unique over other proactive routing protocols.

The use of cognitive with OLSR the two main enhancements are: First is, use OLSR routing protocol, to reduce the possible overhead on the network by MPRs (Multi-point Relays). Second is, with cognitive, the network throughput is increased and reduced congestion delay. In OLSR the packets routed among the shortest path without viewing traffic distribution and load on the paths. Due to this some shortest path nodes have overloaded and then delay can propagate throughout the network.

Some of the shortest paths links are more congested due to congestion the delay propagate on the network. So we will embed cognitive with OLSR to avoid congestion delay because cognitive avoids the congested paths and choose the shortest path from source to destination, it choose the most suitable source to destination path without congested on the network. Cognitive is learning based so it also avoids the path oscillations. Cognitive can find a path with high throughput with same hop count; it does not focus only on shortest path but also with load on the nodes.

In section II, we present a related work. We present proposed work in section III and Conclusion and future work in section IV.

II. RELATED WORK

This section discusses the related works on OLSR and cognitive network and some mechanisms which are applied to reduce the delay and efficient throughput. There are many research papers published regarding to evaluate the performance of the networks. The majority of them distress from packet dropping, congestion on the networks. Following are some of the related works suffering with misbehaviour of the nodes while transferring the data.

Mohamed ELshaikh, Nidal Kamel, Azlan Awang[1]

They proposed an approach, a signal-to-noise ratio (SNR) as a metric to determine the optimum route between source to destination. OLSR is selected for the new metric. A comparison has been made between the conventional hop-count metric and SNR for OLSR routing protocol. They used the metrics for comparison is: network throughput, End-to-End delay, and routing protocol overhead. And Concluded that using SNR as a routing algorithm metric is performing better than the conventional hop-count in WMN environments.

Francesco Saverio Proto, Andrea Detti, Claudio Pisa, Giuseppe Bianchi [2].

Wireless mesh networks built by volunteers which own configure and manage their wireless nodes. Such types of networks are prone to either intentional or unintentional node misbehaviours. They proposed a fully distributed trust-based routing framework, integrated with OLSR. They used the Steganography technique for hidden the active probes in the normal data traffic and Eigen Trust mechanism for path-wide measurement. To determine which packet droppers affects the network forwarding operations. Then the each node trust values transformed into suitable weights as transmitted to the OLSR protocol for mitigating through re-routing. The concluded result, the framework is effective in detecting and circumventing packet-droppers.

Sergio Marti, T.J Giuli, Kevin Lai and, Mary Baker [3]

Two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward the packets but fail to do so. To mitigate this problem, the categorization nodes based on their dynamically measured behaviour. The first technique is watchdog that identifies misbehaving nodes and second is pathrater that helps routing protocol avoid these nodes. The watchdog and pathrater are evaluating using packet throughput, percentage of overhead (routing) transmissions, and accuracy of misbehaving node detection. When used together in a network with moderate mobility, the two techniques increased throughput by 17% in the presence of 40% misbehaving nodes, while increasing the percentage of overhead transmissions from the standard routing protocol's 9% to 17%. During extreme mobility the watchdog and pathrater can increase network throughput by 27%, while increasing the overhead transmissions from the standard routing protocol's 12% to 24%.

A.Venkaiahnaidu,B.RameshBabu,Sk.MansoorRahaman,K .RajaekharaRao[4]

Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol that establishes a route based on a requirement. By avoiding counting-to-infinity problem it performs better when compared to most common routing protocols of the Internet. The AODV cannot capitalize on all available dynamic spectrum resources in cognitive wireless mesh networks yet maintaining a high throughput to route packets. For that reason they propose an enhanced AODV protocol named AODV-COG that provides an interface to a route for efficient usage of the spectrum and finding a path with high throughput among the paths with same hop count. And also focus on Optimized Link State Routing Protocol (OLSR).

Yu Li [5]

Yu Li had had proposed that multi- path routing protocols in wireless mesh networks have much of favour such as fault tolerance, high bandwidth, improved security and better load balance. In wireless mesh networks the reputation-based system using a multi-path routing protocol that stimulates each node in different paths to forward packets from others nodes. The reputation system used to detect misbehaving nodes whose reputation values are below a threshold. Due to this, the reputation system can provide an incentive for misbehaving nodes to behave honestly. And concluded that the reputation system is very efficient in detecting misbehaving node and increase the average throughput of the network.

Sepandar D. Kamvar, Mario T.Schlosser, Hactor Garcia-Molina[6]

In their paper they describe an algorithm to decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network that assigns each peer a unique global trust value, based on the peer's history of uploads.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

They shown a distributed and secure method to compute global trust values, based on Power iteration. By having peers use these global trust values to choose the peers from whom they download, the network effectively identifies malicious peers and isolates them from the network. This reputation system, called Eigen Trust, has been shown to significantly decrease the number of inauthentic files on the network, even under a variety of conditions where malicious peers cooperate in an attempt to deliberately subvert the system.

Dominic C. Follett-Smith[7] in their work they investigates the possibilities of introducing cognition in next generation wireless mesh networks with the expectation of improved performance. It touches briefly on how different definitions of cognitive radio have led to differing communication models and approaches, and there after looks at where there might be scope for further innovation. They discuss cognition in wireless mesh networks is closely cantered around two dominant (and competing) routing protocols: OLSR and B.A.T.M.A.N. Concluded that these is quite promising as an upcoming (and possibly better) alternative in wireless mesh networks.

Sameh R. Zakhary *et.al* [8] in their study shown that with fully distributed reputation-based mechanisms that improve security in MANETS, and introduce a number of optimisations to the current reputation schemes used in MANETs such as selective deviation tests and adaptive expiration timer that aim to deal with congestion and quick convergence. The two different centrality measures for evaluation of the individual trust claims and resolving the aggregated ones. They design and build our prototype over AODV and test it in the NS-2 in the presence of variable black hole attacks in highly mobile and sparse networks. Concluded that increased throughput while delay and jitter decrease and converge to AODV.

III. PROPOSED WORK

The proposed framework is designed by COLSR and two modules, the first is reputed-trust module and second is weighting module. The reputed-trust module built the trust-mechanism of the node in the network and weighting module properly assigns the trust level of nodes to the weight of links of COLSR topology.

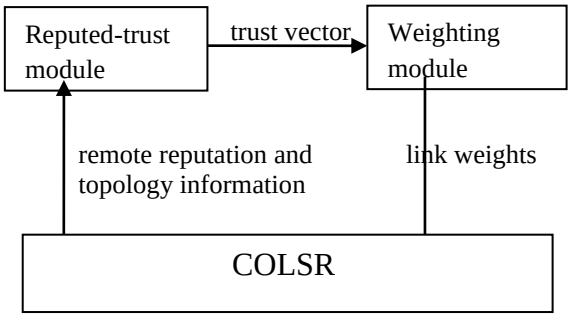

Fig 2. Permit-based COLSR Routing Framework

The reputed-trust module of nodes computes the level of reputation that one node of all other nodes. The source node measures the reputation of a destination node by monitoring the accuracy of data forwarding by destination node and reputed values are measured by source node are collected in a reputation vector and also remote and local reputed vectors are collected, and according to remote and local reputed vectors it measures trust- vector by reputed-trust module. The weighting-module finally assigns the weight to the links and forward to COLSR. The objective of the weighting module is weighting the links on the basis of trust vector values which is calculated by reputed-trust module. And COLSR perform the re-routing so the best route will be followed.

With this framework the data are send between the trusted nodes, no any packet droppers can harm the data and the delay in the network are minimized. So, those nodes that misbehaving either intentionally or unintentionally cannot perform the effect on the network. The packet droppers nodes are avoided to act as intermediate nodes when send the data from source to destination by the COLSR.

IV. CONCLUSION AND FUTURE WORK

In this paper we conclude that when OLSR will implemented, framework is needed for routing the packets, here we use OLSR proactive routing protocol. When packets are transmitted the congestion on the nodes and packet dropping problem are arises. In future, we will work how to remove these problems and enhance the COLSR and implement of COLSR in Wireless Mesh Networks.

REFERENCES

[1] Mohamed ELshaikh et.al:"*High Throughput Routing Algorithm Metric for OLSR Routing Protocol in Wireless Mesh Networks*", 2009 IEEE.
[2] Francesco Saverio Proto et.al:" *A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks*", 2011 IEEE ICC.
[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "*Mitigating routing misbehaviour in mobile ad hoc networks," in MobiCom* '00: Proceedings of the 6th annual international conference on Mobile computing and networking. New York, NY, USA: ACM, 2000, pp. 255–265.
[4] Venkaiahnaidu.A et.al:"*A New OLSR Routing Protocol in Cognitive Wireless Mesh Networks*", IJMER Vol.2, Issue.1, Jan-Feb 2012 pp-496-498.
[5] Yu Li", *A Reputation System for Wieless Mesh Network using Mutli-path Routing Protocol*," 2011 IEEE.
[6] Sepandar D. Kamvar et.al," *The Eigen Trust Algorithm for Reputation Management in P2P Networks*", *WWW2003*, May 20–24, 2003, Budapest, Hungary.
[7] Dominic C. Follett-Smith:"*Smart Wireless Mesh Networking: Introduction coginition in the protocol stack.*"
[8] S. Zakhary and M. Radenkovic, "*Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments*," in Proceedings of WONS 2010, Kranjska Gora, Slovenia, February 2010.
[9] Sonja Buchegger et.al:" *A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Nteworks*- How Much Can Watchdogs Really Do?" 2004 ICC WMCSA.
[10] C. Adjih et.al, "*Attacks against OLSR: Distributed key management for security*," in 2005 OLSR Interop and Workshop, Ecole Polytechnique, Palaiseau, France.
[11] D. Raffo et.al, "*An advanced signature system for OLSR*," in Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04). Washington, DC, USA: ACM Press, October 25 2004, pp. 10–16.
[12] Sepandar D. Kamvar et.al," *The Eigen Trust Algorithm for Reputation Management in P2P Networks*", WWW2003, May 20–24, 2003, Budapest, Hungary.
[13] http://www.ece.gatech.edu/research/labs/bwn/surveys/mesh.pdf.
[14] http://www.justha ckitnow.com

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Manpreet Kaur, Research Scholar, Done M.Sc(CS) from GNDU, Amritsar, now doing M.Tech (CSE) from Lovely Professional University, Phagwara, Punjab, India, Research Area is Wireless Mesh Network.

Kunwarpal, Assistant Professor in Department of Computer Science, Lovely Professional University, Phagwara, Punjab, India, done B.Tech from KMIT Sultanpur, M.Tech from PEC. Research Area is Network.