A SURVEY ON WIRELESS MESH NETWORKS: CURRENT RESEARCH TRENDS

[1]Dr Shajilin Loret J.B, [2]Dr Ganesh Kumar T
[1&2]Assistant Professor,
[1]Department of Computer Science and Engineering,
[1]VV College of Engineering, Tirunelveli, India
[2]Tamizhan College of Engineering and Technology, Kanyakumari, India.

Abstract- Wireless mesh networks have emerged technology for next-generation wireless networking. Because of their advantages over other wireless networks, WMNs are rapid progress and inspiring various applications. However, many technical issues still exist in this field. In the past few years, wireless mesh networks (WMNs) have drawn significant attention from academic and industry as a fast, easy, and economical solution for broadband wireless access. This paper discussed about various routing and scheduling algorithms and the comparison is also performed, And still there are open research issues and that are focused in future.

Index Terms: wireless mesh networks; routing protocols.

I. INTRODUCTION

Wireless mesh network is a communications network made up of radio nodes organized in a mesh topology. Wireless mesh networks often consist of mesh clients, mesh routers and gateways. The mesh clients are often laptops, mobile phones and other wireless communication devices while the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet[1]. A network is a collection of devices that are able to communicate with each other[2]. The networking coverage area of the radio nodes functioning as a single network is sometimes called a mesh cloud. Access to this mesh cloud is dependent on the radio nodes working in harmony with each other to make a radio network. A wireless mesh network is dependable and offers redundancy[3]. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or intermediate nodes. Wireless mesh networks are implemented with different wireless technology including 802.11, 802.16, cellular technologies or combinations of more than one type. It is often assumed that all nodes in a wireless mesh network are immobile but this need not be so. Often the mesh routers are not limited in terms of resources compared to other nodes in the network and thus can be exploited to perform more resource intensive functions. In this way, the wireless mesh network differs from an ad-hoc network since all of these nodes are often constrained by resources[4].

II. ARCHITECTURE

Wireless mesh architecture is providing high-bandwidth network over a specific coverage area. Wireless mesh architectures infrastructure is, in effect, a router network minus the cabling between nodes. It's built of peer radio devices that don't have to be cabled to a wired port like traditional WLAN access points (AP) do. Mesh architecture sustains signal strength by breaking long distances into a series of shorter hops[5][6]. Intermediate nodes not only boost the signal, but cooperatively make forwarding decisions based on their knowledge of the network, i.e. perform routing. Such architecture may with careful design provide high bandwidth, spectral efficiency, and economic advantage over the coverage area[7].
Example of three types of wireless mesh network:
• Infrastructure wireless mesh networks: Mesh routers form an infrastructure for clients.
• Client wireless mesh networks: Client nodes constitute the actual network to perform routing and configuration functionalities.
• Hybrid wireless mesh networks: Mesh clients can perform mesh functions with other mesh clients as well as accessing the network.

Wireless mesh networks have a relatively stable topology except for the occasional failure of nodes or addition of new nodes. The traffic, being aggregated from a large number of end users, changes infrequently. Practically all the traffic in an infrastructure mesh network is either forwarded to or from a gateway, while in ad hoc networks or client mesh networks the traffic flows between arbitrary pairs of node[8][9].

III MANAGEMENT

This type of infrastructure can be decentralized (with no central server) or centrally managed (with a central server), both are relatively inexpensive, and very reliable and resilient, as each node needs only transmit as far as the next node. Nodes act as routers to transmit data from nearby nodes to peers that are too far away to reach in a single hop, resulting in a network that can span larger distances. The topology of a mesh network is also more reliable, as each node is connected to several other nodes. If one node drops out of the network, due to hardware failure or any other reason, its neighbours can find another route using a routing protocol[10].

IV. OPERATION

The principle is packets travel around the wired Internet data will hop from one device to another until it reaches its destination. Dynamic routing algorithms implemented in each device. To implement dynamic routing protocols, each device needs to communicate routing information to other devices in the network.. The routing algorithm used should attempt to always ensure that the data takes the most appropriate (fastest) route to its destination[11].

V. MULTIRADIO MESH NETWORKS

Multi-radio mesh refers to a unique pair of dedicated radios on each end of the link. This means there is a unique frequency used for each wireless hop and thus a dedicated CSMA collision domain. This video applications work as they would on a wired Ethernet network. In true 802.11 networks, there is no concept of a mesh. There are only Access Points (AP's) and Stations. So a Multi-radio wireless mesh node will dedicate one of the radios to act as a station, and connect to a neighbor node AP radio. Single and dual-radio mesh use proprietary means to repeat the signal in the same collision domain and frequency. That is what causes bandwidth degradation and high latency[5].

IV.ROUTING PROTOCOLS

Three backward path routing protocols such as reactive hop-by-hop routing (AODVCGA), proactive hop-by-hop routing (FBR), and proactive source routing (GSR). One major difference between GSR and the other two protocols is that with GSR, all routing state information is kept on the mesh gateways, while with the other two protocols; the state information is distributed on the mesh nodes. Furthermore, GSR re-uses forward paths collected by data packets while the other protocols depend on dedicated routing control packets to determine routes[12].

IV.REACTIVE HOP-BY-HOP ROUTING (AODV-CGA)

We can use an extended version of AODV for wireless mesh networks. This extension extends the AODV routing domain to include a network border router that is connected to all gateways. Upon receiving a packet from the Internet addressed at a mesh node, the border router floods a route request to all gateways from where a route is then determined in the mesh network[13].

V. GATEWAY SOURCE- ROUTING(GSR)

A source routing protocol that re-uses the forward paths that are recorded by data packets and stored on the gateways. These paths are then used for source routing on the backward path[12].

VI.GSR- PN(ENHANCEMENT FOR PERFORMANCE)

The GSR protocol is designed for scalability to the network size. However, its packet delivery ratio drops rapidly if feedback packets do not frequently update the routes. Such link breaks happen mostly between nodes that are almost at the maximal transmission range to each other. In order to reduce the probability of mobility-induced link breaks, preferred neighbor (PN) mechanism is proposed to GSR that is similar to the mechanism[12].

GSR is scalable to the network size and has no route set-up delay. Find that if the receiver sends a feedback packet towards the Internet host every five seconds, the packet delivery ratio remains high, even in scenarios where nodes move at car speed. With an enhanced version called GSR-PN, a higher packet delivery ratio in highly mobile scenarios. That gateway source routing is a promising routing approach, since in our study, it delivers the best trade-off between packet delivery ratio, routing overhead, and scalability to the network size[12].

VII.OPTIMIZED LINK STATE- ROUTING PROTOCOL

A signal-to-noise ratio (SNR) is a metric to determine the optimum route between source and destination. Optimized Link State Routing Protocol (OLSR) is selected for the new metric. The network throughput, End-to-End delay and routing protocol overhead are used for performance metrics for the comparison between three protocols (AODV, DSR, and OLSR) .

Network throughput: When there are many number of nodes there will be of low performance measure. However, when the mobility scenario is applied, the DSR has the highest throughput among the other protocols[14].

VII.INTELLIGENT PORTAL ROUTING ALGORITHM

Intelligent Portal Routing Algorithm **(**IPRA), a hybrid routing algorithm for wireless mesh networks. In IPRA, the mesh portal broadcasts periodically a mesh update message which populates the route towards the mesh portal in the routing table for each of the mesh points. IPRA also allows the use of intelligent mesh portals and mesh points to further improve the performance of mesh network.The packet delivery ratio using IPRA is the same for all “Network Update” intervals in static scenarios and is higher than in AODV. The routing overhead incurred with IPRA protocol is lower than that of AODV. The main reason for the lower overhead is that in IPRA the routes to the mesh portal are semi-permanent with no expiration timer, thus the nodes do not need to re-broadcast the route request after every route expiration period.IPRA algorithm, the end-to-end delay for the packet is considerably reduced for all the static scenarios and the scenarios with low mobility. This reduction of delay is due the fact that, with the semi-permanent routes towards the mesh portal, the data packet is sent immediately in IPRA. In pure AODV, the data packet is first buffered, then the route request is sent and subsequently the data packet is transmitted when the node gets the route reply[15].

In scenarios with high mobility, the end-to-end delay is a function of mesh update interval. With higher interval for mesh updates, the delay is comparable to AODV, since the mesh points would send the route request in the event of link breakages which are frequent in high mobility scenarios. With high intervals for mesh updates however, the fresh routes are maintained very frequently thus allowing the nodes to have newer and better routes if there is a link breakage. In high mobility scenarios, with high intervals for mesh updates, the threshold for transmitting route request is quite low and consequently the delay increases[16].

VII.SPLIT MULTIPATH ROUTING

A.Route Discovery

Split Multipath Routing (SMR) is an on-demand routing protocol that builds multiple routes using requestheply cycles. When the source needs a route to the destination but no route information is known, it floods the ROUTER REQUEST(RREQ) message to the entire network. Because this packet is flooded, several duplicates that traversed through different routes reach the destination. The destination node selects multiple disjoint routes and sends ROUTE REPLY (RREP) packets back to the source via the chosen routes[17].

B.RREQ Propagation:

The main goal of SMR is to build *maximally disjoint multiple paths. T*o construct maximally disjoint routes to prevent certain nodes from being congested and utilize the network resources efficiently. To achieve this goal in on-demand routing schemes, the destination must know the entire path of all available routes so that it can select the routes. The source routing approach where the information of the nodes that consist the route is included in the RREQ packet. If nodes reply from cache as in DSR and AODV, it is difficult to establish maximally disjoint multiple routes because not enough RREQ packets will reach the destination and the destination node will not know the information of the route that is formed from the cache **of** intermediate nodes.[17]

VIII.MULTICAST ALGORITHMS (LCA & MCM)

The Level Channel Assignment (LCA) algorithm and the Multichannel Multicast (MCM) [9] are to progress the throughput for multichannel and multi-interface mesh networks. An efficient multicast trees by minimizing the number of relay nodes and total hop count distances of the trees. These algorithms used channel assignment strategies to reduce the interference to improve the network capacity.LCA algorithm is to improve system throughput. First, LCA cannot diminish the interference among the same levels since it uses the same channel at the same level. Second, when the number of available channels is more than that of the levels, some channels will not be utilized, which is a waste of channel diversity. Third, the channel assignment does not take the overlap property of the two adjacent channels into account[18].

IX.LOAD- AWARE ROUTING SCHEME

In a WMN, the traffic load tends to be unevenly distributed over the network. A routing scheme is proposed which maximizes the utility, i.e., the degree of user satisfaction, by using the dual decomposition method. With this scheme, a WMN is divided into multiple clusters for load control[19][20]. A cluster head estimates traffic load in its cluster. As the estimated load gets higher, the cluster head increases the routing metrics of the routes passing through the cluster. Based on the routing metrics, user traffic takes a detour to avoid overloaded areas, and as a result, the WMN achieves global load balancing. This scheme effectively balances the traffic load and outperforms the routing algorithm using the expected transmission time (ETT) as a routing metric[21].

X. SCHEDULING ALGORITHM NOVEL SCHEDULING ALGORITHM

A novel scheduling algorithm is a quality-driven cross-layer design framework to jointly optimize the parameters of different network layers to achieve highly improved video quality for P2P video streaming applications in multi-hop wireless mesh networks. The quality driven P2P scheduling algorithm is formulated into a distributed distortion-delay optimization problem. The distributed optimization running on each partner node adopted in the scheduling algorithm greatly reduces the computational intensity[22].

XI.ROUTING TREE PROBLEM

Wireless Internet-access Mesh Network (WIMNET) is composed of multiple access points (APs) that are connected with each other by wireless communications. At least one AP performs as the gateway (GW) to the Internet. Any host in the network can access to the Internet through this GW, after associating its neighbor AP and communicating with multihop wireless links between APs. The delay along the routing path degrades the performance of WIMNET. To avoid the bottleneck of communications by minimizing the maximum delay, the routing tree problem is formulated for AP communications, and it proves the NP-completeness of its decision version. Then, the greedy heuristic algorithm of sequentially selecting one link is proposed that minimizes the delay of the predicted tree containing the link[23].

XII.ADAPTIVE SPLIT TRANSMISSION ALGORITHM

Adaptive split transmission algorithm is to distribute real-time and quality-guaranteed video flows in wireless mesh networks. It is only employed by the mesh nodes that are going to suffer from overload. During the procedure of the split transmission[24], the mesh node $v(r)$ checks the original channel that was used to transmit. When the channel status becomes light loaded, $v(r)$ stops splitting the video flow and transmits the whole basic layer through the original channel instead. Therefore, the occupied multiple channels can be released and then used by other mesh nodes. This algorithm fully and efficiently utilizes the unused capacities and non-interfering simultaneous transmission of multiple channels attaching to different individual radio interfaces. Without conducting complex channel hopping and assignment, the algorithm aggregates unused channel capacities to transmit a basic layer video flow when its transmission may cause overload in individual channels the *adaptive split transmission algorithm* holds the following characters[25].

- Pro-activity. The *overload detection* for the algorithm that detects a coming overload in some channel based on the flow input rate. Therefore, traffic control can be implemented before overload occurs which greatly decreases the possibility of unacceptable performance.
- Adaptively. Mesh nodes employ the *adaptive split transmission algorithm* under heavy load network status adaptively. The algorithm enables the basic layer video to transmit through adaptively splitting the traffic into several sub-flows whose transmission rates suitable for channels' unused capacities.
- Efficiency. By efficiency, That the number of subflows is small and the packet delays are short. As few as possible channels that have enough aggregative capacities are selected to transmit short delay sub-flows. To keep the number of selected channels small is to enable other flows to have opportunity to use channels and also decrease the number of generated sub-flows which is good for continuous and light overhead communications.
- Deployability: The proposed algorithm can inter-operate with current available hardware and MAC protocols without modification, and existing upper-layer protocols including current work on multiple channels. Therefore, the algorithm doesn't complicate wireless systems and is readily deployed using current commodity wireless mesh equipments[24].

XIII.AUTOREGRESSIVE INTEGRATED MOVING AVERAGE

Network traffic is predicted based on past data using ARIMA mode, and provide that input to the routing and scheduling algorithm. Joint routing and scheduling results are in significant performance improvement over the routing algorithms. So, predicted network traffic information to a joint routing and scheduling algorithm known as Traffic Oblivious routing and scheduling. Traffic Oblivious Routing and Scheduling algorithm optimizes the worst case performance under traffic uncertainty but when accurate traffic information is available to the algorithm, its performance is enhanced. In the Traffic Oblivious Routing and Scheduling algorithm, computing the routing and the scheduling values is a one time overhead[26].

XIV.LINK-STATE ALGORITHMS

When applying link-state algorithms, each node uses as its fundamental data a map of the network in the form of a graph. To produce this, each node floods the entire network with information about what other nodes it can connect to, and each node then independently assembles this information into a map. Using this map, each router then independently determines the least-cost path from itself to every other node using a standard shortest paths algorithm such as Dijkstra's algorithm. The result is a tree rooted at the current node such that the path through the tree from the root to any other node is the least-cost path to that node. This tree then serves to construct the routing table, which specifies the best next hop to get from the current node to any other node[27].

XV.OPTIMIZED LINK STATE ROUTING ALGORITHM

A link-state routing algorithm - optimized for mobile ad-hoc networks is the *Optimized Link State Routing Protocol (OLSR)*. OLSR is proactive, it uses Hello and *Topology Control* (TC) messages to discover and disseminate link state information into the mobile ad-hoc network. Using Hello messages each node discovers 2-hop neighbor information and elects a set of *multipoint relays* (MPRs). MPRs make OLSR unique from other link state routing protocols. Individual nodes use the topology information to compute next hop paths regard to all nodes in the network utilizing shortest hop forwarding paths[28].

XVI.PATH VECTOR PROTOCOL

Distance vector and link state routing are both intra-domain routing protocols. They are used inside an autonomous system, but not between autonomous systems. These routing protocols become intractable in large networks and cannot be used in Inter-domain routing. Distance vector routing is subject to instability if there are more than a few hops in the domain. Link state routing needs huge amount of resources to calculate routing tables. Path vector routing is used for inter-domain routing. It is like to distance vector routing. In path vector routing assume there is one node in each autonomous system which acts on behalf of the entire autonomous system. This node is called the speaker node. Path vector routing is discussed in RFC 1322; the path vector routing algorithm is somewhat similar to the distance vector algorithm in the sense that each border router advertises the destinations it can reach to its neighboring router. However, instead of advertising networks in terms of a destination and the distance to that destination, networks are advertised as destination addresses and path descriptions to reach those destinations[29].

XVI.MESH SECURITY

The conventional WLAN security mechanisms (e.g., such as WPA2/802.11i) provide standardized methods for authentication, access control and encryption between a wireless client and an access point. Since most wide-area mesh solutions strive to retain compatibility with commercial off-the shelf WLAN client adapters, existing standardized WPA2 mechanisms are commonly retained[30]. However, there are many different types of wireless mesh architectures, where each type of architecture may use a different approach for wireless security. Many approaches for mesh security may be derived from ad-hoc security research, but any future commercial mesh products will standardize security through 802.11s.

XVII.SECURITY ATTACKS OF WMN

In this section, the main threats that violate the security criteria, which are generally known as security attacks, are analyzed.

A. Major Attack Types of WMN

There are various kinds of attacks in wireless mesh network. The main types of attack are briefly described as follows.

B. Denial of Service attack

The DoS attack is encountered either by accidental failure in the system or a malicious action. The conventional way to create a DoS attack is to flood any centralized resource so that it no longer operates correctly or stop working. A distributed DoS (DDoS) attack is an even more severe threat to WMNs. DDoS attack is launched by a group of compromised nodes who are part of the same network and who collude together to bring the network down or seriously affect its operation. One instance of DoS attack is SYN flooding.

C. Impersonation attack:

This attack creates a serious security risk in WMNs. If proper authentication of parties is not supported, compromised nodes may be able to join the network, send false routing information, and masquerade as some other trusted nodes. A compromised node may get access to the network management system of the network; and it may start changing the configuration of the system as a legitimate user who has special privileges. Security mechanism of impersonation attacks could be to apply strong authentication methods in contexts where a party has to be able to trust the origin of data it has received or stored.

D. Routing attack:

Routing attacks in WMNs could be:

Routing table overflow attack - an attacker attempts to create routes to nonexistent nodes with intention to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. This attack could also lead to a resource exhaustion or DoS attack.

.*Wormhole attack* - an attacker receives packets at one location in the network and tunnels them selectively to another location in the network. Then, the packets are resent into the network, and the tunnel between two colluding attackers is referred to as a wormhole.

Blackhole/sinkhole attack - a malicious node uses the routing protocol to advertize itself as having the shortest path to the node. In this situation, the malicious node advertize itself to a node that it wants to intercept the packet.

Byzantine attack - an invalid operation of the network initiated by malicious nodes where the presence of compromised nodes and the compromised routing are not detected. This attack will eventually result in severe consequences to the network as the network operation may seem to operate normal to the other nodes.

XVIII. CONCLUSION

WMNs can be built up based on existing technologies, field trials and experiments with existing WMNs prove that the performance of WMNs is still far below expectations. As explained throughout this paper, there still remain many research problems. Among them, the most important and urgent ones are the scalability and the security.

XIX. REFERENCE

[1] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless mesh networks: a survey,” *Comput. networks*, vol. 47, no. 4, pp. 445–487, 2005.

[2] S. Radley, D. Krishnamoorthy, U. Ivy, B. Persis, and others, “Routing Virtualization for IPv4-IPv6 Coexistence By Means of Real Time Simulation,” 2017.

[3] D. Rahbari, “Hybrid evolutionary game theory in QoS routing of wireless mesh networks,” *Int. J. Comput. Sci. Telecommun.*, vol. 4, no. 9, 2013.

[4] A. Raniwala and T. Chiueh, “Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network,” in *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, 2005, vol. 3, pp. 2223–2234.

[5] N. R. Nomulwar, J. N. VarshaPriya, B. B. Meshram, and S. T. Shinghade, “Comparision of performance of routing protocol in Wireless Mesh Network,” *Int. J. Comput. Sci. Appl.*, vol. 1, 2012.

[6] S. M. A. Al Subail, S. M. M. Ahsan, and M. Enayetullah, “Development of A New Efficient Routing Scheme for WiMAX Mesh Networks,” *Int. J. Mod. Educ. Comput. Sci.*, vol. 5, no. 10, p. 27, 2013.

[7] J. Ellis, C. Pursell, and J. Rahman, *Voice, video, and data network convergence: architecture and design, from VoIP to wireless*. Academic Press, 2003.

[8] P. E. Rod Mahdavi, “Data Center Energy Efficiency Measurement Assessment Kit Guide and,” 2012.

[9] D. Krishnamoorthy, S. Chidambaranathan, and others, “Clever Cardnovel Authentication Protocol (NAUP) in Multi-Computing Internet of Things Environs,” 2017.

[10] N. T. Patil, “Secure Transmission in Ad-hoc Network: Using Combined Cryptography.”

[11] X. Hong, K. Xu, and M. Gerla, “Scalable routing protocols for mobile ad hoc networks,” *IEEE Netw.*, vol. 16, no. 4, pp. 11–21, 2002.

[12] R. Baumann, S. Heimlicher, V. Lenders, and M. May, “Routing packets into wireless mesh networks,” in *Wireless and Mobile Computing, Networking and Communications, 2007. WiMOB 2007. Third IEEE International Conference on*, 2007, p. 38.

[13] L. M. L. Oliveira, A. F. De Sousa, and J. J. P. C. Rodrigues, “Routing and mobility approaches in IPv6 over LoWPAN mesh networks,” *Int. J. Commun. Syst.*, vol. 24, no. 11, pp. 1445–1466, 2011.

[14] M. E. M. Campista, P. M. Esposito, I. M. Moraes, L. H. M. K. Costa, O. C. Duarte, D. G. Passos, C. V. N. De Albuquerque, D. C. M. Saade, and M. G. Rubinstein, “Routing metrics and protocols for wireless mesh networks,” *Network, IEEE*, vol. 22, no. 1, pp. 6–12, 2008.

[15] R. Zoican, “Adaptive routing with intelligent portal in wireless mesh networks,” in *Computational Technologies in Electrical and Electronics Engineering, 2008. SIBIRCON 2008. IEEE Region 8 International Conference on*, 2008, pp. 395–398.

[16] A. Damle, D. Rajan, and S. M. Faccin, “Hybrid routing with periodic updates (HRPU) in wireless mesh networks,” in *Wireless Communications and Networking Conference, 2006. WCNC 2006. IEEE*, 2006, vol. 1, pp. 318–324.

[17] S.-J. Lee and M. Gerla, “Split multipath routing with maximally disjoint paths in ad hoc networks,” in *Communications, 2001. ICC 2001. IEEE International Conference on*, 2001, vol. 10, pp. 3201–3205.

[18] L. Zhao, A. Y. Al-Dubai, and G. Min, “GLBM: A new QoS aware multicast scheme for wireless mesh networks,” *J. Syst. Softw.*, vol. 83, no. 8, pp. 1318–1326, 2010.

[19] M. Salem, “Radio Resource Management in OFDMA-based Cellular Relay Networks,” *Dr. Philos. Electr. Eng. Carlet. Univ.*, 2011.

[20] D. Krishnamoorthy, D. Ramya, Y. Rajkumar, U. Ivy, B. Persis, S. Kavitha, and others, “A Novel Approach towards Lowest Energy Usage Routing Protocol (LEuRP) in Wireless Mobile Ad-Hoc Network (WMANet),” 2017.

[21] K. W. Choi, W. S. Jeon, and D. G. Jeong, “Efficient load-aware routing scheme for wireless mesh networks,” *IEEE Trans. Mob. Comput.*, vol. 9, no. 9, pp. 1293–1307, 2010.

[22] M. Asefi, J. W. Mark, and X. S. Shen, “A mobility-aware and quality-driven retransmission limit adaptation scheme for video streaming over VANETs,” *IEEE Trans. Wirel. Commun.*, vol. 11, no. 5, pp. 1817–1827, 2012.

[23] N. Funabiki, “Access-Point Allocation Algorithms for Scalable Wireless Internet-Access Mesh Networks,” in *Wireless Mesh Networks*, InTech, 2011.

[24] W. Tu and C. J. Sreenan, “Adaptive split transmission for video streams in wireless mesh networks,” in *Wireless Communications and Networking Conference, 2008. WCNC 2008. IEEE*, 2008, pp. 3122–3127.

[25] M. D. Schroeder, R. M. Needham, C. P. Thacker, A. D. Birrell, T. L. Rodeheffer, E. H. Satterthwaite Jr, and H. G. Murray Jr, “High-speed mesh connected local area network.” Google Patents, 1992.

[26] C. Wang, Z. Lu, Z. Wu, J. Wu, and S. Huang, “Optimizing Multi-Cloud CDN Deployment and Scheduling Strategies Using Big Data Analysis,” in *Services Computing (SCC), 2017 IEEE International Conference on*, 2017, pp. 273–280.

[27] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, *A scalable content-addressable network*, vol. 31, no. 4. ACM, 2001.

[28] M. Benzaid, P. Minet, K. Al Agha, C. Adjih, and G. Allard, “Integration of Mobile-IP and OLSR for a Universal Mobility,” *Wirel. Networks*, vol. 10, no. 4, pp. 377–388, 2004.

[29] X. Masip-Bruin, M. Yannuzzi, J. Domingo-Pascual, A. Fonte, M. Curado, E. Monteiro, F. Kuipers, P. Van Mieghem, S. Avallone, G. Ventre, and others, “Research challenges in QoS routing,” *Comput. Commun.*, vol. 29, no. 5, pp. 563–581, 2006.

[30] D. Krishnamoorthy and others, “Optimal Path Selection in Mobile Adhoc Networks for Time Sensitive Applications,” 2017.