INJ INTERNATIONAL NEUROUROLOGY JOURNAL

Design & development of testing, evaluation of different types of routing protocols & effectiveness for low power lossy networks

Dr. Mamatha C.M., Anupriya A.G., Swathi V
Professor and Head, Dept. of Computer Science & Engineering (CY),
Cambridge Institute of Technology North Campus, Bengaluru, Karnataka
Assistant Professor, Department of Computer Science & Engineering,
Cambridge Institute of Technology North Campus, Bengaluru, Karnataka
Assistant Professor, Department of Computer Science & Engineering,
Cambridge Institute of Technology North Campus, Bengaluru, Karnataka

Abstract

The Internet of Things (IoT) involves expanding the Internet's capacity to gather, analyze, and share data for creating information. IoT devices enable direct connections to form intelligent and self-aware environments. Low Power Lossy Networks (LLNs), particularly the Routing Protocol for LLNs (RPL), serve as the IoT foundation. This study focuses on RPL's architecture and protocol stack, evaluating its performance in a simulated Smart Health scenario. Additionally, it compares reactive protocols (DSR and AODV) and a proactive protocol (DSDV) in mobile Adhoc networks, considering factors like throughput and delay. Another aspect explores routing protocols for Low-power and Lossy Networks in Smart Grids, comparing RPL and LOAD. The article also assesses routing protocol performance under diverse traffic conditions, such as CBR, FTP, and TELNET, in MANETs. Lastly, the study evaluates routing protocols (RIP, OSPF, IGRP, EIGRP) for public safety networks, considering convergence, throughput, and queuing delay. The simulation results guide the selection of appropriate protocols for specific applications.

Key Words: WSN, PDF,,AODV, QOS, LVMP.

Introduction

Enhanced information sharing enhances interoperability for public safety organizations, resulting in higher-quality services for the public. The central computer network is vital for communication and information exchange in public safety operations. Despite budget constraints, effective routing protocols are crucial to ensure the functionality of networks, especially when utilizing older equipment. Choosing the right routing protocol, such as OSPF for large networks and EIGRP for medium to large networks, is essential for optimal performance. This study focuses on modeling a mission-critical public safety network connecting two towns, emphasizing the Emergency Communications Center as the main hub. The network utilizes FDDI for node connections. The schematic diagram in Fig. 1 illustrates the AODV path finding process.

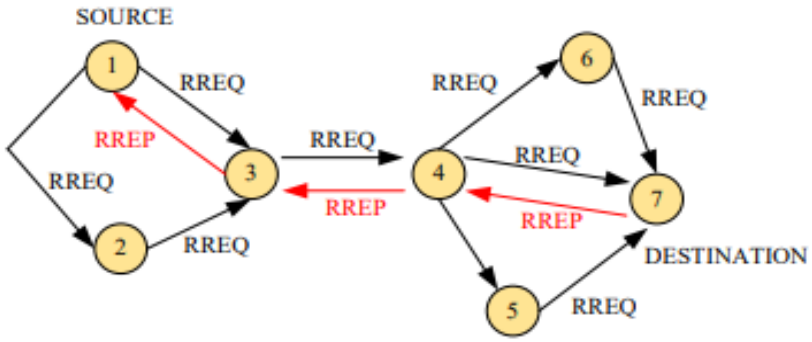

Fig. 1 : Schematic diagram of AODV path finding process

RPL establishes a Directed Acyclic Graph (DAG) by linking node attributes and link costs, incorporating factors like energy resources, workload, throughput, latency, and dependability. The objective function in RPL provides flexibility in minimizing costs to reach any sink, aligning closely with IPv6 architecture. Signaling messages in IPv6 Router Advertisements maintain the gradient in RPL. ER-RPL, designed for P2P communications, utilizes region data crucial for static networks like M2M systems and WSNs, enabling effective routing pathways based on location information. In contrast, geographic routing relies on node locations for data forwarding, using either actual or virtual coordinates. While offering low routing overhead and scalability, geographic routing may

struggle with consistent data delivery in lossy wireless networks, often requiring constant neighbor database exchanges. The Fig. 2 illustrates the flow chart of DSR route discovery.

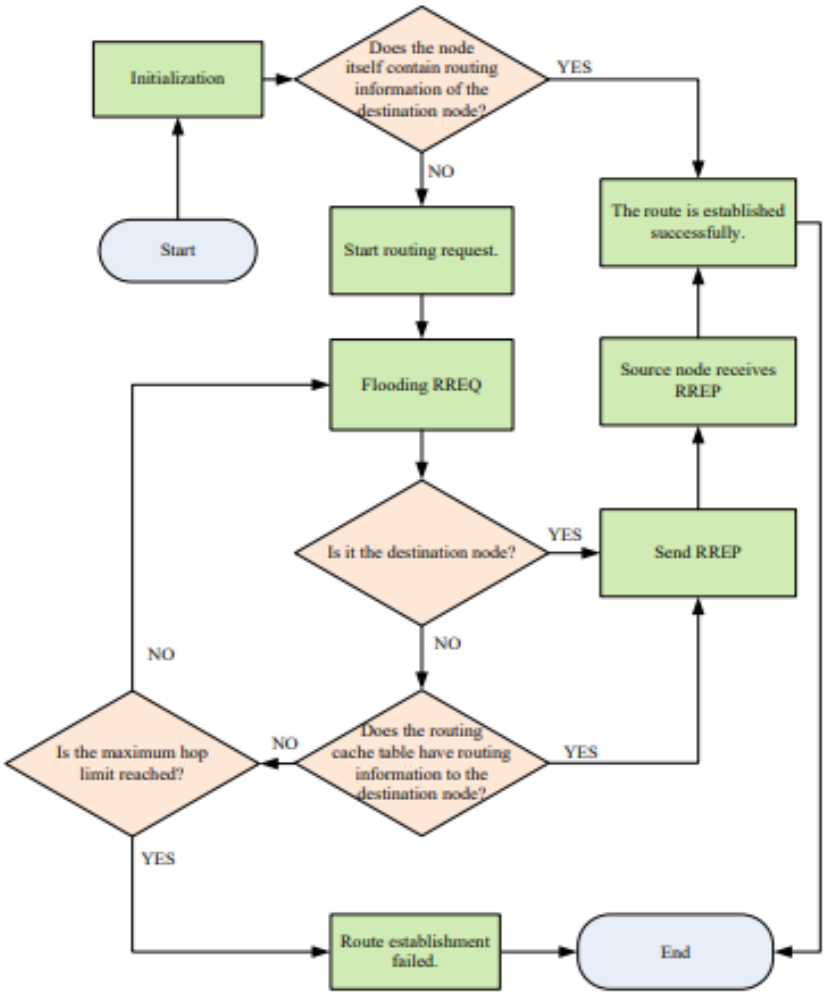

Fig. 2 : The flow chart of DSR route discovery.

In a resource-constrained network, energy usage can be a significant cost factor. The Self-Regioning method maintains uniform node density in each zone, enabling nodes to create multiple regions based on proximity to Reference Nodes (RNs). With adaptations for various geometries, such as four regions in a rectangular area and six in a hexagon-shaped zone, the method generates octagonal regions with additional neighbor RNs and two areas per RN with nearby RNs. Incorporating more RNs results in 2N regions when NRN/s are present. ER-RPL optimizes P2P route selection, reducing control overhead with additional RNs. During region-based route discovery, nodes in IRCM regions select optimal routes, transferring routing information near the source or destination nodes. The DODAG root facilitates communication between source and destination node regions. Nodes maintain R2R tables, and layer triggers, like the Obvious Cramming Announcement method, aid in identifying network congestion. Coat gun trigger techniques offer optimization by taking a perpendicular crosscut across layers. Cross-layer interaction addresses issues in TCP performance in multi-hop IEEE 802.11v networks, with suggested solutions like the TCP fractional window increment scheme and route-failure notification using bulk-loss trigger policy.

In recent years, wireless mesh networks (WMNs) have gained increasing attention and installation rates, with numerous successful mesh firms providing equipment and solutions. IEEE 802.11s standardizes network mesh WLANs, while IEEE 802.15.5 focuses on network meshing for wireless private part networks, and IEEE 802.16j defines wireless multi-hop relaying. WMNs offer superior performance, flexibility, and reliability compared to traditional wireless LANs. Effective routing protocols in WMNs adapt to dynamic network topology changes, facilitating communication between nodes through multiple wireless hops. While MANET-specific routing techniques are often applied in WMNs, the two share fundamental concepts with differing

emphasis, as MANETs originated from academia and WMNs from a commercial background. The terms WMNs and MANETs are used interchangeably to highlight their close relationship. Notably, wireless mesh networks are widely used for public WIFI access, with access points distributed in cities, campuses, and corporate locations, providing customizable backhaul. This study delves into the field of radio network systems, specifically summarizing routing in WMNs and discussing the future IEEE 802.11s WLAN mesh networking standard based on the March 2006 draft standard D0.01.

Related Works – Literature Review

This paper delves into various research studies focused on routing protocols and their performance in different network scenarios. The first study assesses routing protocols for UAV communication networks, emphasizing the challenge of reliable information transmission in low-altitude situations. The second study explores the IoT and RPL routing protocol, evaluating its potential in a Smart Health setting. The third study compares reactive (DSR, AODV) and proactive (DSDV) protocols in mobile ad hoc networks (MANETs), highlighting the importance of careful protocol selection. The fourth study analyzes routing protocol performance in wireless mesh networks, considering proactive and reactive methods under different traffic conditions.

In the fifth study, the RPL routing protocol is scrutinized for its applicability in wireless sensor networks, emphasizing its quick network setup but suggesting improvements in protocol overhead. The sixth study evaluates routing protocols for low-power and lossy networks, specifically comparing Loading and RPL, considering resource demand, traffic patterns, and routing overhead. The seventh study proposes ER-RPL, an energy-efficient region-based routing protocol for low-power and lossy networks, outperforming benchmark protocols in simulations. The eighth study focuses on routing protocols in an Emergency Communications Center, emphasizing the importance of choosing the right protocol for mission-critical scenarios.

The ninth study shifts attention to FANETs, evaluating routing protocols (AODV, DSDV, DSR, OLSR) based on metrics like throughput, end-to-end latency, and node count. The tenth study assesses the objective functions in the IPv6 routing protocol for LLNs in IoT applications, comparing MRHOF and OF0 performance. The eleventh study reviews current routing protocols for ad hoc mobile wireless networks, categorizing and comparing table-driven and on-demand schemes. The twelfth study surveys protocols and standards for the Internet of Things, highlighting the importance of standards for IoT ecosystem development.

The thirteenth study describes proposed routing for IEEE 802.11s WLAN mesh networks, providing insights into the planned routing protocols based on the draft standard. The fourteenth study introduces a protocol for intercommunication in packet network protocols, focusing on end-to-end error checking, sequencing, and flow control. The fifteenth study compares the QoS-PAR routing procedure with AODV in radio communication ad hoc networks, emphasizing the former's performance under increasing network size and flow count.

The sixteenth study investigates routing protocols and security issues in wireless sensor networks, analyzing various routing methods and addressing security risks. The seventeenth study evaluates routing protocols for MANETs under different traffic conditions, comparing AODV, DSR, and WRP for CBR, FTP, and TELNET traffic. The eighteenth study implements the DSDV routing protocol for wireless mobile ad-hoc networks, comparing its performance with DSR and AODV under varying scenarios. The nineteenth study reiterates the focus on routing protocols in an Emergency Communications Center, comparing convergence, throughput, and queuing time for four different protocols.

The twentieth study proposes a routing protocol for cloud networks, addressing the challenges of communication in wireless cloud environments and comparing the efficiency of different routing protocols. Collectively, these studies provide a comprehensive overview of routing protocols in diverse network scenarios, contributing valuable insights for network design and optimization.

Research Methodology Adopted

Regarding packet forwarding, the node exhibits egocentric behavior, indiscriminately dropping every received packet, whether it is a data packet or a routing packet. This egocentric behavior leads to a lower packet delivery ratio and consequently lower throughput on nodes characterized by increased selfishness. While there is a trend for delay reduction, it is expected that delays will escalate if routing packets are lost. The quicker the packet is discarded, the smaller the latency, compared to the value observed in a healthy network. Figure 8 illustrates the structure of the UAV communication network simulation system.

These performance indicators are notably affected by the prevalence of selfish nodes, as fewer packets translate to reduced network congestion, and swifter packet delivery implies enhanced overall performance. Among the three protocols examined, AODV exhibits a superior packet delivery rate. Suspicion about network activity results in increased routing burden, with egotistical nodes discarding more routing packets than AODV, which responds promptly to network changes and generates a higher number of control packets. OLSR and DSDV, both transmitting periodic updates, convey an identical quantity of routing information irrespective of the network state. Consequently, a discernible decline in conventional statistics volume leads to an increase in routing overhead. However, this escalation is not a direct response of the protocol to potential attacks. In this uncommon scenario, the reactive AODV protocol outperforms the others.

DSR functions as a reactive source routing system designed for ad hoc networks, accommodating up to 200 mobile nodes. Differing from other unicast routing protocols, DSR does not uphold a routing database but rather relies on the source routing option in data packets. It employs a Route Cache that maintains an extensive list of IP addresses for each node along the path to the target. Essentially, if a route to the destination is cached, route discovery is unnecessary; however, if the cache lacks a route to the destination, broadcasting a route request message initiates the route discovery process, with the source receiving a response to the route request.

AODV routing technology is built upon the foundations of DSR and DSDV, integrating the DSR-like route finding process and the episodic beaconing and order enumeration of DSDV. Despite these similarities, AODV and DSR exhibit two key distinctions. AODV sends packets with only the destination address, leading to potentially lower routing overheads compared to DSR, which transmits packets with full routing information. AODV's route replies contain only the sequence number and destination IP address, whereas DSR's route replies encompass the addresses of all nodes along the route. AODV's adaptability to highly dynamic networks is advantageous, but it may face delays and increased bandwidth use in route construction and rerouting, contributing to elevated network congestion as the network expands.

Comparing the results across publications is challenging due to differing test settings and protocol aspects. Instead, a summary and comparison of the routing protocols DSDV, DSR, and AODV are provided. Uniformly dispersed CBR sources with random waypoints serving as the mobility model are used in all investigations. Throughput, often referred to as packet delivery fraction, is assessed based on the quantity of minutes communicated between sources and destinations per unit of time or the ratio of delivered packets. Figure 3 illustrates the node model of UAV in this context.

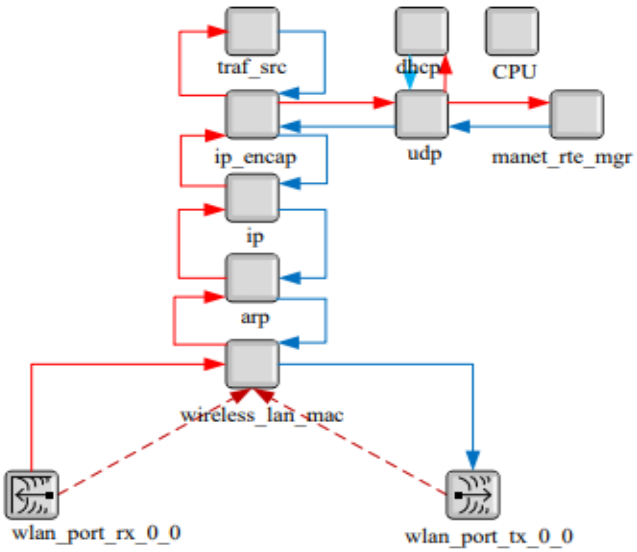

Fig. 3 : The node model of UAV.

An excess of Constant Bit Rate (CBR) packets contributes to increased delays, particularly notable when traffic congestion arises. Delay at low flexibility is more pronounced than at moderate mobility due to heightened delays from increased mobility and traffic loads. Congestion, stemming from multiple flows routed through a single network area, is a primary cause. DSR exhibits the highest average delay, showing shorter delays under low loads but inferior performance under high loads where AODV excels. The growing number of nodes,

however, adversely impacts DSDV's performance as node mobility escalates, leading to increased routing table exchanges.

Routing overhead, denoting the total quantity of packets for routing transmitted over the network, rises in tandem with growing mobility. AODV, owing to numerous route replies to a single route request, incurs higher routing overhead than DSR. DSDV's routing overhead is influenced by its continuous route updates constrained by a per-node transmission period, rendering it constant and independent of mobility. The serial number in the topology control (TC) group facilitates the separation of old and new routing data, enabling random updates and transmission of TC packets. The ongoing interaction between TC packets establishes one-hop and two-hop neighbor node information, maintaining the wireless ad hoc network's topology. Multipoint Relay (MPR) technology, employed in the OLSR protocol, selects relay nodes building symmetric links with all two-hop neighbor nodes, drastically reducing the volume of TC packets sent over the network. In this approach, a one-hop neighbor node, upon receiving a broadcast packet, determines whether it is the node's MPR node, forwarding the packet if affirmative. This technique reduces control packet length and minimizes connections needed for control message transmission. In the IEEE 802.11s update, a new category of mesh management for action management frames is defined, with the action field's value determining the type of management message to be sent, displayed as an IEEE 802.11 information element as shown in the Figs. 4, 5 & 6 respectively.

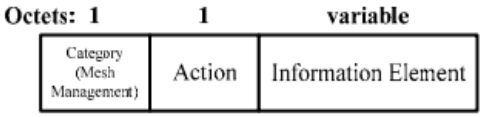

Fig. 4 : IEEE 802.11s mesh management action frame format

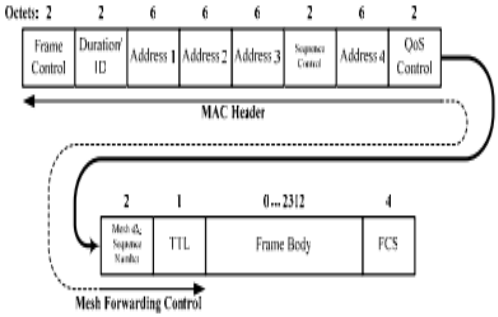

Fig. 5 : IEEE 802.11s mesh data frame format

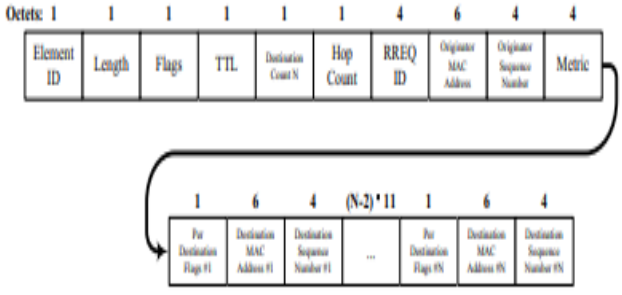

Fig. 6 : Structure of HWMP route request (RREQ) information element

Figures 4, 5, and 6 illustrate the IEEE 802.11s mesh management action frame format, IEEE 802.11s mesh data frame format, and the structure of HWMP route request (RREQ) information elements. Reactive routing's primary advantage lies in determining a path only when necessary for data transmission between mesh nodes. Initial packet delay occurs as path computation and connection discovery start after the first data packet reaches the routing module of the base node. In the absence of mesh network traffic or static traffic patterns, on-demand path generation utilizes the latest link status data, reducing routing overhead. The route-finding mechanism, akin to AODV and DSR, involves broadcasting a route request message from a foundation mesh point to reach a last-stop mesh point. Each mesh point processes and transmits the route request, and intermediate mesh points send unicast route reply messages to construct the path to the destination. The route-finding technique is updated to

comply with IEEE 802.11s path selection protocol requirements, incorporating layer 2 MAC addresses and radio-aware connection metrics.

The reactive routing mechanism of Hybrid Wireless Mesh Protocols (HWMP) is elaborated further. If a path to the source mesh point S already exists, the mesh point assesses whether an update is necessary. The path to S changes if the new path metric in the RREQ surpasses the metric in the associated routing table entry, and the RREQ's sequence number equals or exceeds the sequence number in the current routing table entry for S. Modification of the existing path occurs regardless of the new path metric value if the RREQ's sequence number is higher than the linked routing table item by at least a specified threshold value.

HWMP facilitates simultaneous path discovery to multiple destinations using a single Route Request (RREQ) message. The destination count parameter within the RREQ indicates the number of destination mesh points to be discovered. Destination count sequences include details such as turfs per destination, destination discourse, and terminus arrangement quantity. To accommodate variations in control flags for different destinations in the RREQ, the flags are divided into two groups. Matching per destination flags fields are set independently for each destination, ensuring accurate path metric data by traversing the entire path with both route demand and route account.

The flags field, containing control flags uniform for all destinations in the RREQ, defaults to broadcast (UB = 1) for the unicast/broadcast flag (UBv), introduced for HWMP proactive extensions. HWMP utilizes an arbitrary link metric, often a radio-aware one like the default airtime link metric, instead of the hop total steering measure. The hop count field in the RREQ message indicates the number of relations in the trail but isn't used for routing decisions. Initial values for both the hop count and metric are set to 0, and the RREQ's range is specified in hops through the time to live field (TTL). Before generating a new route request, the source mesh point's RREQ ID counter is incremented. If the route request is for route discovery, the sequence number of the source mesh point (originator) is increased by 1.

In July 2004, the IEEE 802.11v working group's research group for ESS mesh networking was renamed task group "s" (TG's) with the aim of creating a versatile and extendable wireless mesh network standard based on IEEE 802.11v. IEEE 802.11s focuses on radiocommunication multi-hop routing for radiocommunication promotion. The PAR document defines the scope and some specifications of IEEE 802.11s, referring to mesh nodes as mesh points (MPs). A station supporting both IEEE 802.11v and mesh is termed a mesh point, and "mesh capabilities" in the context of the proposed 802.11s amendment pertain to contributing to the net steering etiquette and advancing information on behalf of other net facts, as depicted in Figure 8 as the net grid.

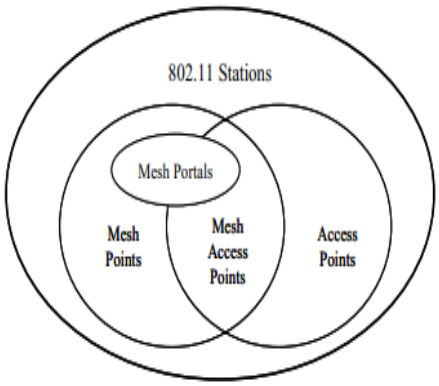

Fig. 7 : Relation amongst diverse IEEE 802.11 (mesh) nodes.

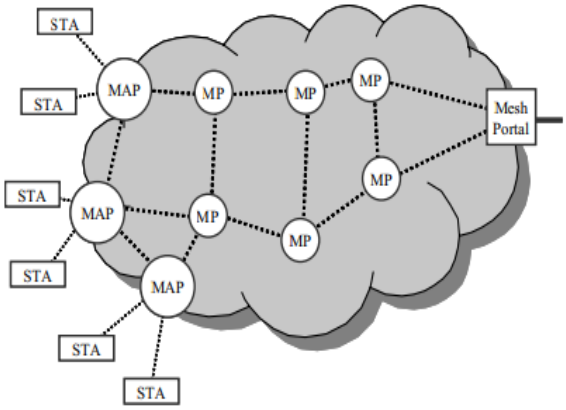

Fig. 8 : Example of an IEEE 802.11s WLAN net system

Simulation Results

Simulations are performed & the results are observed. The Fig. 9 gives the average throughput for different routing protocols. (a) The number of nodes is 20 , the UAV speed is 10m/s (b) The number of nodes is 20, the UAV speed is 20m/s. (c) The number of nodes is 40, the UAV speed is 10m/s. (d) The number of nodes is 40, the UAV speed is 20m/s.

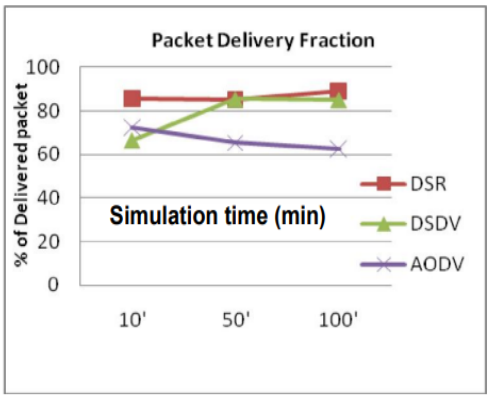

Fig. 9 : Packet Delivery Fraction-1

Conclusions

The study comprehensively evaluated routing protocols for various network scenarios, emphasizing their crucial role in systems like autonomous vehicles (AV), public safety networks, IoT, and Low-Power and Lossy Networks (LLNs). In the AV system, EIGRP emerged as the superior protocol, surpassing RIP, OSPF, and IGRP. Despite FDDI's obsolescence, EIGRP stood out due to minimal latency, making it the preferred choice even for financially constrained public safety groups. Shifting focus to IoT protocols, the document covered layers such as information joining, system direction-finding, system encapsulation, and session layers. It highlighted protocols standardized by IETF, IEEE, ITU, and ongoing developments, providing a valuable resource for developers and service providers navigating the complex IoT protocol landscape. Security concerns, ongoing standardization efforts, and management protocols were also briefly addressed.

Exploring IEEE 802.11s, the extensible framework for routing, the study outlined its versatility with RA-OLSR as an optional protocol and configurable default routing protocol HWMP. Acknowledging the evolving nature of the draft standard, the study stressed the solid foundation of the routing system while anticipating adjustments during the standardization process. Finally, the examination of routing protocols within LLNs offered crucial insights, revealing performance variations influenced by network size, density, and topology. Energy efficiency, scalability, fault tolerance, security, and standardization emerged as critical considerations. The conclusions drawn provide a basis for future research, guiding the development of resilient, energy-efficient, and scalable routing solutions tailored to the unique challenges of LLNs and contributing to the advancement of communication in this evolving field.

References

1. Z. Jose, V.V. Sobral Joel, J.P.C. Rodrigues Ricardo, A.L. Raelo, Jalal Al-Mutadi & Valery Korotaev, ”Routing protocols for low power & low power and lossy networks in internet of things applications”, 9 May 2029.
2. Karim Rostamzadeh, Hasen Nicanfar, Narjes Torabi, Sathish Gopalakrishnan, Victor C.M. Leung, “A Context aware trust based information dissemination framework for vehicular networks”, IEEE Internet of Things Transactions, Vol. 2, No. 2, Apr. 2015.
3. Z. Safdar, S. Farid, M. Pasha, K. Safdar, “A security model for the IoT based systems”, Technical Journal, Univ. of Engg. & Tech. (UET), Taxila, Pakistan, Vol. 22, No. 4, ISSN : 1813-1786, 2017.
4. Shubhalika Dihulia, Tanveer Farooqui, “A survey on IoT security Challenges”, Int. Journal of Comp. Appliances, ISSN : 0975-8887, Vol. 169, No. 4, Jul. 2017.
5. Vandana Sharma, Ravi Tiwari, “Security on IoT & its smart appliances”, Int. Jour. of Science, Engg. & Tech. Research (IJSETR), Vol. 5, Issue 2, Feb. 2016.
6. Sachin Updadhya, “Ongoing challenges & research opportunities”, Int. Jour. of Engg. Technologies & Management Research, Vol. 5, No. 2, Special Edition, pp. 216-222, DOI : 10.6281/Zefnodo.1195065
7. Wei Zhou, Yuging Zhang, Peng Liu, “Effect of IoT new features on security & privacy”, The college of Info. Sciences & Tech., The Pennsylvania State Uni., PA, 16802, USA.
8. Saeed Banaeian Far Azadeh Imani Rad, “Security analysis of Big Data on IoT”, IEEE Transactions in Industrial Electronics, Vol. 12, Issue 3, ISSN : 1232-1242, 2016.
9. Mirza Abdur Razzaq, Mohammed Ali Qureshi, Sajid Habib Gill, Saleem Ullah, “Security issues in IoT”, IJASCA, Int. Jour. of Adv. Comp. Sci. & Appliances, Vol. 8, No. 6, 2017.
10. Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, “A review on security in IoT”, 2012 IEEE Int. Conf. of Comp. Sci. & Engg., 2012.
11. Xiaopeng Tan, Zhen Zuo, Shaojing Su, Xiaojun, Guo, Xiaoyong Sun, Deng Jiang. “Performance Analysis of Routing Protocols for UAV Communication Networks”, IEEE Access, 2020.
12. Accettura, Nicola, Maria Rita Palattella, Mischa Dohler, Luigi Alfredo Grieco, and Gennaro Boggia, “Standardized power efficient & internet-enabled communication stack for capillary M2M networks”, 2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2012.
13. Zheng Min Wang, Wei Li, Hui Liang Dong, “Analysis of Energy Consumption and Topology of Routing Protocol for Low-Power and Lossy Networks”, Journal of Physics: Conference Series, 2018.
14. Md Anam Mahmud, Ahmed Abdelgawad, Kumar Yelamarthi, “Improved RPL for IoT Applications”, 2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS), 2018
15. Kumar, Neeraj, and Mayank Dave, “A Beacon Information Independent VANET Routing Algorithm with Low Broadcast Overhead”, International Journal of Computer Network and Information Security, 2015.\
16. Michael Bahr, “Proposed routing for IEEE 802.11s WLAN mesh networks”, Proceedings of the 2nd annual international workshop on Wireless internet – WICON’06, 2006
17. Ivascu, G.I., “QoS routing with traffic distribution in mobile ad hoc networks”, Computer Communications, 20090212
18. Xiongwei Ren, Jianqi Zhang, “Review of the Cross-Layer Design in Wireless Ad Hoc and Sensor Networks”, 2010 International Conference on Computational Intelligence and Software Engineering, 2010.
19. Watteyne, T., & Pister, K. S. (2011). "Stress testing the Internet of Things: The mctest framework." In 2011 8th IEEE International Conference on Mobile Ad-Hoc and Sensor Systems (MASS) (pp. 529-534).
20. Dohler, M., Watteyne, T., Winter, T., & Barthel, D. (2012). "Towards a reliable internet of things: A survey." Journal of Sensor and Actuator Networks, 1(2), 101-139.
21. Gnawali, O., Fonseca, R., Jamieson, K., Moss, D., & Levis, P. (2009). "Collection tree protocol." In Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems (SenSys) (pp. 1-14).
22. Duquennoy, S., Al Nahas, B., Landsiedel, O., & Johansson, P. (2013). "Let the tree bloom: Scalable opportunistic routing with ORPL." In Proceedings of the 11th ACM Conference on Embedded Networked Sensor Systems (SenSys) (pp. 1-14).
23. Hui, J. W., Culler, D., Chakrabarti, S., & Levis, P. (2008). "The dynamic behavior of a data dissemination protocol for network programming at scale." In Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems (SenSys) (pp. 81-94).
24. Thubert, P., & Watteyne, T. (2016). "Industrial Routing Requirements in Low-Power and Lossy Networks." RFC 7774, Internet Engineering Task Force (IETF).

25. Brandt, A., Buron, J., & Toutain, L. (2014). "Survey of Routing in Low Power and Lossy Networks: Background and Overview." RFC 6553, Internet Engineering Task Force (IETF).