OPTIMIZING NETWORK COMMUNICATION: ROUTING PROTOCOL PERFORMANCE IN THE IOT

Hitesh Parmar[1], Dr. Kamaljeet lakhtariya[2]

[1]Faculty, M.Sc-IT(CA & IT), K.S School of Business Management & Technology, Gujarat University, Ahmedabad, Gujarat

[2]Associate professor, Department of computer science, Gujarat university, Ahmedabad, Gujarat

Abstract

The IoT is the networking of a large number of interrelated objects, which requires the implementation of efficient routing protocols. The article is mainly concerned with the evaluation of the performance of AODV, DSR, OLSR, and TRPL, referred to as the main routing protocols for the IoT environments, and parameters such as overhead, load, delay, and throughput are used to do this. The author makes use of NS2 to expose how these protocols perform under different network scenarios, and this research pointed out that the performance of each protocol differs across different kinds of topologies and levels of mobility. AODV is known to have lower delay and overhead, which makes it the preferred option for time-critical situations, whereas OLSR achieves higher throughput, which is of particular benefit for data-intensive situations. DSR works fine, except it cannot achieve dynamic topologies as efficiently as those with protocols that provide basic IP. TRPL asserts a trust-based scheme by adding a new technique for security communications in the field of IoT. Consequently, the results suggest that no one protocol as a whole might outperform others over time, but elements such as the size of the network, mobility in the mesh nodes, and data pattern in the IoT application should be determinants of the selection of a suitable protocol. In future studies, reliance on innovative methods that merge the best aspects of current approaches and the adoption of security technologies that address the unique challenges of IoT are vital.

Key Terms: IoT, AODV, Routing Protocols, OLSR, TRPL

Introduction

With the launch of the IoT, the world is in a new technological era where there is a massive device network that communicates and shares data. This flourishing network seeks to simplify our lives and streamline our routines to suit our needs. In contrast to that, the multiplicity of IoT devices is one of the problems, the other being different network connectivity needs, which may turn out to be a cumbersome challenge, especially in terms of network routing. Efficient routing protocols are indispensable prerequisites of effective and reliable linkages, as they aim to keep the amount of consumed energy at the minimum possible level and enhance the

network's overall functionality. This paper outlines the efficiency characteristics of widely known routing mechanisms for IoT implementations, which provide the groundwork for the communication solution in the presently used, complex environment.

The IoT networks consist of a high-level and fast-changing number of devices that require robust routing protocols that will do the necessary communication management directly from a wide range of devices with different capacities and requirements. Traditional routing protocols, namely AODV, DSR, and OLSR, have been exhaustively studied with the purpose of improving their performance under different network conditions, which provides some valuable findings for the comparison of various routing protocols for MANETs and WSNs (Liu et al., 2017). Nevertheless, these protocols are in need of periodic viability evaluation and even the need for relevant adaptation to the specific difficulties presented by the IoT ecosystem that imply device heterogeneity, energy use limitations, and communication scalability and security.

It is energy technology that becomes a critical factor in IoT network systems, where battery life is often the main difference between them. The reviews of Awais et al. (2019) and Kalidoss et al. (2019) have clearly indicated the critical role of designing efficient pathways and mechanisms that can bring down the energy consumption of the networks, noting that the smart implementation of energy-aware and neuro-fuzzy-based routing algorithms has the potential to extend network lifespan. Moreover, data transmission should be reliable and secure, considering it could involve informative data or safeguard critical operations (Mao et al., 2019; Abbasi et al., 2018). ZTRPL, as a trust-based protocol, opens the way for the building of trust in IoT secure communications through the use of trust metrics, which are used to evaluate and select routing paths (Sobral et al., 2019).

Scalability is considered a factor where routing protocols are concerned, as more devices connect to the existing ones. The performance of the protocols needs to be such that they can cope with the expansion of the network without an exponential drop in performance. The attempt to address the research by Safaei et al. was randomly undertaken.

Statement of the Problem

The case of IoT networks is very pluralistic. They consist of many gadgets, which can be either static or mobile. Their creativity reaches the limits of the universe and their energy levels. The traditional protocol types, which were centred around homogeneous and stationary networks, are usually not good enough to meet the symmetrical environment of an IoT formed by individual devices, various protocols, and different capabilities. The main obstacle is to create routing protocols capable of managing high variability in device mobility, density, and energy resources, ensuring secure, reliable, and timely data transmission. These protocols, which

were developed by Awais et al. (2019) and Mao et al. (2019), might be useful. Besides the scalability of these protocols, this issue, which is gaining wide popularity, remains critical in such a way that the IoT network keeps growing exponentially.

Objective

The aim of this research is to present an in-depth consideration of four engagement protocols, namely: AODV, DSR, OLSR, and TRPL within IOT. Therefore, the study will not only recognise the key features of each protocol but also identify their constraints. It is based on the result of this analysis that the most suitable routing methods are going to be selected for IoT applications; thus, the network size, node mobility, and application requirements, among others, are going to be taken into account.

Associated Works

The IoT has been incrementally increasing its presence in technological domains and contributing to key areas such as healthcare, agriculture, and smart cities with billions of connected devices that help achieve inter-mesh connectivity. This giant network, beyond anything able to meet these requirements, needs to be purposefully designed for automation and efficiency and then concede unique security challenges such as networking and data routing. The related works in this area of IoT networking show the current intention to solve these issues through the creation and optimisation of relevant routing algorithms that fit the innovative IoT environments.

Awais et al. (2019) unveiled the underwater WSNs, disclosing methods to fill the gap and improve energy utilisation through the deployment of proactive routing protocols. Their job highlights the need for properly managing energy sources, which for IoT devices function well under not-so-good conditions. As Mao et al. (2019) present, the team aims to improve the reliability of data transmission between IoT devices by designing a DTN probabilistic router. This research will contribute to scheduling because its objective is to improve the overall efficiency of IoT networks. Such scheduling will be particularly successful in scenarios where real-time conventional communication protocols may present shortcomings.

The concern by Kalidoss et al. (2019) passes onto consideration of the deployment of energy-efficient clustering and neurofuzzy-based routing algorithms, which have been applied to wireless sensor networks. The ways they go about noting this show the ability to mesh artificial intelligence techniques with traditional routing protocols and, as a result, the improvements in terms of IoT network efficiency and adaptability. The combination of AI and network principles will be an exemplary application of the IoT routing protocols of the future, designed to be dynamic enough and diverse enough to meet the fast-growing demand for IoT device communication.

Furthermore, the authors have also reported that they compared four different routing protocols in the nested network: AODV, DSR, OLSR, and DSDV, in which the DSDV algorithm for every node was designed to maintain a stable long-distance relationship. The results present essential characteristics of these protocols, which are safety and risk factors, forming the basis for tailoring and improving these protocols in the IoT era. The work's research promotes the necessity of investigating the distinct structural behaviours of the protocols and the different issues that arise in the IOT network domains to make sure that the protocols are well suited and can function faultlessly for each specific situation.

Methodology

The evaluation methodology used in our study fits the most important activity routing protocol versions—OLSR, DSR, AODV, and TRPL—being comparatively evaluated for an IoT context. Thought to be done is a crucial element for moving to the next phase, which concerns the tuning of the TCP/IP protocol requirements to deal with the diversity and fluctuations of the IoT network environment. The frequency of the examination included showing the simulation of the NS2 network simulator. The NS2 network simulator can often be found in the networking field, as it is powerful and informative.

Simulation Setup

The NS2 simulation takes off by creating the bedrock on which our experimental structure is built, and imitation of multiple network configurations is only possible due to the grounding technique used.

What has been established is a virtual network that will be configured to contain a certain number of nodes. These numbers can, in turn, be changed to represent a range of different network configurations, such as network size or density. These nodes, having IoT characteristics like low computing capacity and power scarcity, are deployed to faithfully resemble the specificities of real IoT devices.

Protocol Configuration

The routing protocols, namely “Optimised Link State Routing (OLSR), Dynamic Source Routing (DSR), Ad hoc On-Demand Distance Vector (AODV), and Trust-based Routing Protocol (TRPL)”, are configured in the NS2 environment. For each protocol, its default parameters are adjusted by the degrees to which they can match the common environment, where typical IoT deployment conditions are taken into consideration, in order to angle towards a simulation of the real application scenario.

Evaluation Metrics

Routing Overhead: The routing metric specified above measures the volume of extra network traffic that is transmitted by the said protocol and related to the upkeep of routes. It plays a critical role as an accuracy coefficient, especially in bandwidth-limited networks.

Throughput: Throughput can be used to show the percentage of data that is successfully made to reach its destination within the network. The level of throughput observed is indicative of a protocol's ability to thoroughly utilise network resources and to guarantee accurate transmission of data, which are fundamentally responsive and reliable operations of any IoT application.

End-to-End Delay: This onemetric catches the length of the time within which a data package is en route from its original source to its final destination. One instance is the application of smart grids and the networks of autonomous vehicles.

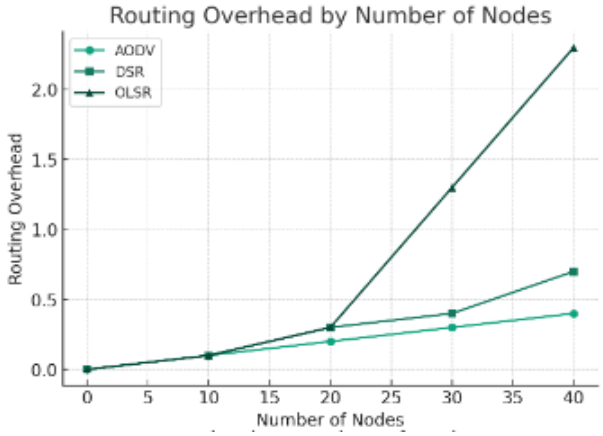
Experimental Scenarios

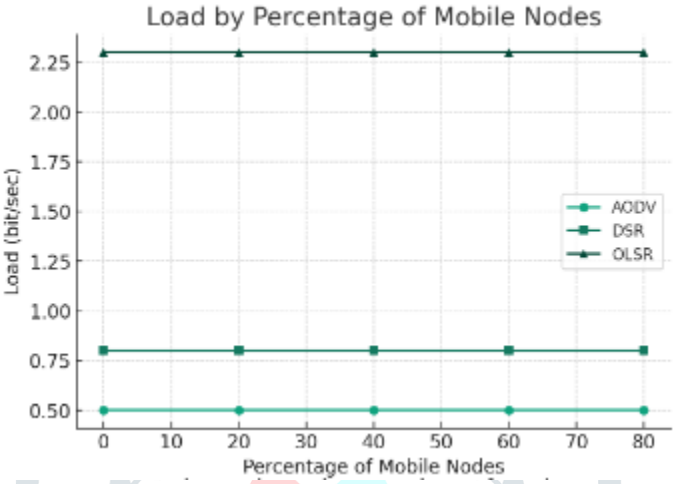
The simulation experiments are dedicated to sweeping the network conditions, pushing the adaptability of each routing protocol and immersion into its function adequately. Using these conditions includes using the number of node changes to represent the network sizes of different nodes and also modifying the rate of moving the mobile nodes to compare the mobility patterns of IoT devices. This approach permits a systematic understanding of the protocol's performance by means of comparison with other milestones, which are crucial factors for its application in Internet of Things frameworks.

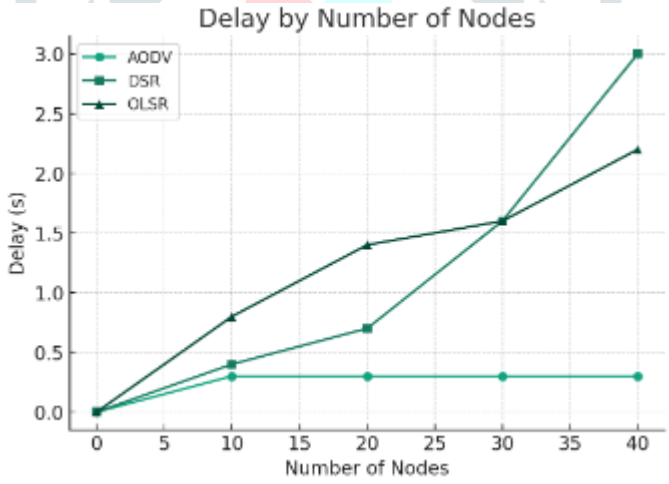
Data Analysis

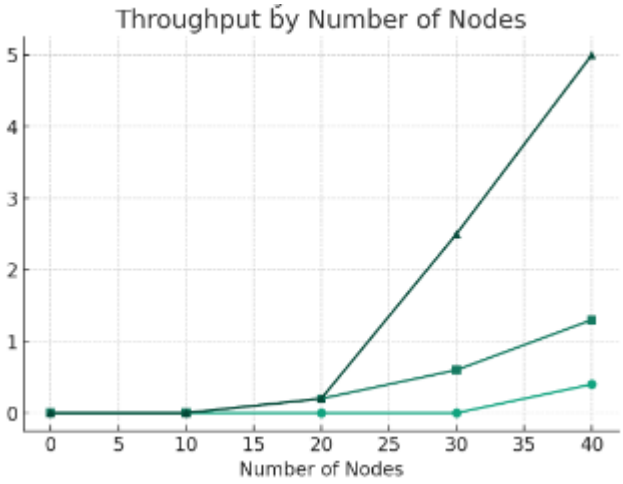
The data are undergoing rigorous analysis to identify the assigned trends and whether they exhibit sufficient differences in performance between the protocols. The server tools that involve statistical measures and graphic representations are used, which result in adequately explaining the impact of networking conditions on the police reports, making it easier to understand some strengths and limitations of the procedure in the case of IoT networking.

Experimental Results









Visualisations of the research results have been presented in form tables and scatter plot graphs, showing the AODV, DSR, and OLSR routing protocols features under various network conditions, with such aspects as routing overhead, load, delay, and throughput included.

Table 1: Routing Projection of Protocols

Nodes Count	AODV	DSR	OLSR
0	0	0	0
10	0.1	0.1	0.1
20	0.2	0.3	0.3
30	0.3	0.4	1.3
40	0.4	0.7	2.3

AODV provides an approximate straight-line growth in sink nodes as the size increases to the value of 0 to 0.4. DSR demonstrated a positive rise for the most part, with a noticeable effect at the fourth level; the overhead amounts to an equivalent value of 0.7. There are two principal causes of the overhead of OLSR: at first, an edge one that is most prominent at large node numbers and peaks at 2.3 given that there are 40 counting nodes running the algorithm.

Table 2: Load of Protocols

Mobile Nodes %	AODV	DSR	OLSR
0%	0.5	0.8	2.3
20%	0.5	0.8	2.3
40%	0.5	0.8	2.3
60%	0.5	0.8	2.3
80%	0.5	0.8	2.3

The traffic load for AODV stays at 0.5 bit/sec for all cases where the percent of mobile NATs is changed. DSR, just like that, runs at 0.8 bit/sec. Although mobile percentage modification has no effect on the

overall mobile node traffic, OLSR has a 2.3-bit/sec data rate at any speed, which is a lot larger than what other protocols might exhibit.

Table 3: Delay of Protocols

Nodes Count	AODV	DSR	OLSR
0	0	0	0
10	0.3	0.4	0.8
20	0.3	0.7	1.4
30	0.3	1.6	1.6
40	0.3	3	2.2

The delay time of AODV is constantly 0.3 seconds for systems and networks with either a small or large node count. All this causes a higher DSR delay as the number increases, which makes up up to 3 seconds at around 40 nodes. OLSR faces a long delay, which values to more than 2.2 seconds for 40 nodes.

Table 4: Delay of Various Protocols

Mobile Nodes %	AODV	DSR	OLSR
0%	0.4	2.8	2.8
20%	0.4	2.8	3.2
40%	0.4	2.8	2.1
60%	0.4	2.8	2.7
80%	0.4	2.8	2.3

AODV has constantly given the same latency (0.4 seconds) regardless of the mobile node proportion. Single-hop protocols (DSR and OLSR) show in general equal delays to 20% nodes, then decrease to 2.2 seconds at the last point.

Table 5: Throughput of Various Protocols

Nodes Count	AODV	DSR	OLSR
0	0	0	0
10	0	0	0
20	0	0.2	0.2
30	0	0.6	2.5
40	0.4	1.3	5

The throughput of AODV does not reach its maximum level of zero until it passes through the 40-node mark at 0.4. In the DSR model, we see increases in throughput, with an actual value of 1.7 at 40 nodes being achieved.

Table 6: Throughput of Various Protocols

Mobile Nodes %	**AODV**	**DSR**	**OLSR**
0%	0.1	1.4	5.1
20%	0.1	1.4	5.1
40%	0.1	1.4	5.1
60%	0.1	1.4	5.1
80%	0.1	1.4	5.1

World throughput, network throughput, and in particular the highest node count, are higher for OLSR than for TFRC, which is up to 5.AODV, while doing so, provides a stable data rate of 0.1 of a bit per second in all of the chosen mobility levels. DSR has its overlay maintenance operations augmented to facilitate a throughput level of 1.4 that is not affected by the proportion of mobile nodes. As it relates to throughput, OLSR exhibits all mobility percentages that indicate the efficiency of handling mobile nodes, displaying a more than desirable result of 5.1.

These charts provide the structure of the routing overhead, the weight of the traffic, the delay, and the performance under different network conditions for AODV, DSR, and OLSR protocols, reflecting the performance inclusive of these factors for the IoT ecosystem in a quantitative frame.

Discussions

Routing Overhead: According to Table 1 and Figure 2, there is additional potential for OLSR overload upon adding the nodes with regards to their larger network management. This leads to less efficiency by OLSR.

Load: Table 2 and Figure 3 indicate that, just in cases where mobile devices are the majority, OLSR load is higher; thereby, OLSR can be thought to be designed to accommodate highly mobile IoT environments.

Delay: Tables 3 and 4 and Figures 4 and 5 exhibit evidence that OLSR always has larger lag times, especially in the overcrowded Internet of Things networks, while AODV ensures low latency and might for future time-constrained IoT applications.

Throughput: Additionally, OLSR can be seen to have an edge in terms of throughput, specifically in scenarios with a high number of nodes or high mobility, based on the data provided in Tables 5 and 6 and Figures 6 and 7, thus showing that it is effective in data-intensive applications.

Conclusion

The simulated performance analysis shows that none of the designed routing protocols produces an overall improvement in all the analysed scenarios within the Internet of Things environment. AODV looks

promising for applications where the network delay is of low importance and where the implementation of overhead is low. DR serves its purpose if the network topology does not change often, whereas OLSR presents itself as the best option when high throughput and stability are needed. TRPL, as a trust-inspired technology, provides an innovative solution to the question of how to secure IoT communications on the internet.

Future Work

The opening of adaptive protocols that can automatically adapt their parameters dependent on the network conditions to be implemented could immensely improve the communicability of IoT. Another area that needs further attention is the protocols that are designed for the security and reliability issues that pose a significant problem for IoT networks; hence, the need has arisen to combine machine learning algorithms for the purpose of predicting network changes and responding with preventative measures.

Reference

1. Abbasi, S., Akram, A., Mushtaq, S., & Azad, A. (2018). Can BATMAN Replace RPL for IoT Applications. *International Journal of Computer Applications*, 180, 32-37. https://doi.org/10.5120/IJCA2018916394.
2. Al-Abdi, A., Mardini, W., Aljawarneh, S., & Mohammed, T. (2019). Using of multiple RPL instances for enhancing the performance of IoT-based systems. *Proceedings of the Second International Conference on Data Science, E-Learning and Information Systems*. https://doi.org/10.1145/3368691.3368718.
3. Awais, M., Javaid, N., Rehman, A., Qasim, U., Alhussein, M., & Aurangzeb, K. (2019). Towards Void Hole Alleviation by Exploiting the Energy Efficient Path and by Providing the Interference-Free Proactive Routing Protocols in IoT Enabled Underwater WSNs. *Sensors (Basel, Switzerland)*, 19. https://doi.org/10.3390/s19061313.
4. Daud, S., Gilani, S., Riaz, M., & Kabir, A. (2019). DSDV and AODV Protocols Performance in Internet of Things Environment. *2019 IEEE 11th International Conference on Communication Software and Networks (ICCSN)*, 466-470. https://doi.org/10.1109/ICCSN.2019.8905256.
5. Dhtore, V., Verma, A., & Thigale, S. (2019). Energy Efficient Routing Protocol for IOT Based Application. *Techno-Societal 2018*. https://doi.org/10.1007/978-3-030-16848-3_19.
6. Hamrioui, S., Hamrioui, C., Díez, I., Lorenz, P., & Mauri, J. (2018). Improving IoT Communications Based on Smart Routing Algorithms. *2018 IEEE Global Communications Conference (GLOBECOM)*, 1-6. https://doi.org/10.1109/GLOCOM.2018.8647183.
7. Kalyani, S., & Vydeki, D. (2018). Measurement and Analysis of QoS Parameters in RPL Network. *2018 Tenth International Conference on Advanced Computing (ICoAC)*, 307-312. https://doi.org/10.1109/icoac44903.2018.8939052.

8. Kalidoss, T., Kulothungan, K., Rajasekaran, L., Selvi, M., Ganapathy, S., & Kannan, A. (2019). Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Comput. Networks*, 151, 211-223. https://doi.org/10.1016/J.COMNET.2019.01.024.
9. Liu, X., Sheng, Z., Yin, C., Ali, F., & Roggen, D. (2017). Performance Analysis of Routing Protocol for Low Power and Lossy Networks (RPL) in Large Scale Networks. *IEEE Internet of Things Journal*, 4, 2172-2185. https://doi.org/10.1109/JIOT.2017.2755980.
10. Mao, Y., Zhou, C., Ling, Y., & Lloret, J. (2019). An Optimized Probabilistic Delay Tolerant Network (DTN) Routing Protocol Based on Scheduling Mechanism for Internet of Things (IoT). *Sensors (Basel, Switzerland)*, 19. https://doi.org/10.3390/s19020243.
11. Okaile, M., Sangodoyin, A., Ramajalwa, R., & Tshepo, M. (2017). Performance Analysis of AODV Routing Protocol Under Blackhole Attack With Sink Shifting. *ZICT Journal*, 1, 47-50. https://doi.org/10.33260/ZICTJOURNAL.V1I1.25.
12. Quy, V., Ban, N., Nam, V., Tuan, D., & Han, N. (2019). Survey of Recent Routing Metrics and Protocols for Mobile Ad-Hoc Networks. *J. Commun.*, 14, 110-120. https://doi.org/10.12720/jcm.14.2.110-120.
13. Safaei, B., Salehi, A., Shirbeigi, M., Monazzah, A., & Ejlali, A. (2019). PEDAL: power-delay product objective function for internet of things applications. *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*. https://doi.org/10.1145/3297280.3297565.
14. Sobral, J., Rodrigues, J., Rabêlo, R., Saleem, K., & Kozlov, S. (2019). Improving the Performance of LOADng Routing Protocol in Mobile IoT Scenarios. *IEEE Access*, 7, 107032-107046. https://doi.org/10.1109/ACCESS.2019.2932718.
15. Zhang, F., Joe, I., Gao, D., & Liu, Y. (2016). A Simulative Study on the Factors Affecting Single-copy and Multi-copy Protocols in DTN. *Computer Engineering*, 16-20. https://doi.org/10.14257/ASTL.2016.123.04.