INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY SCIENCES AND ENGINEERING, VOL. 14, NO. 2, APRIL 2023

Evaluation of RPL-based IoT Protocol Performance under Various Mobility Scenarios

Rimsha Fayyaz[1]**, Nimra Khan**[2]**, Muhammad Haris**
[1-3]Department of Computer Science, University of Engineering and Technology Lahore, Pakistan
[1]mishafayyaz@gmail.com, [2]nimrainamkhan@gmail.com, [3]muhammadharisashfaq@gmail.com

Abstract—**The growth of IoT applications and connected smart devices has made routing a challenging concept. To address this, the IPv6 Routing Protocol for Low-power and Lossy Networks (RPL) was standardized for IoT networks. However, RPL was designed for stationary IoT applications and has difficulty adapting to the dynamic fluctuations of mobile applications. While several studies have attempted to adjust RPL for mobile IoT applications, a standardized version of this protocol is still in high demand. This research presents a comprehensive study on the impact of various mobility models on the performance of a mobility aware RPL to facilitate this process. A performance evaluation is conducted using IoT simulation tools to compare the performance of the network and its IoT devices under different mobility models from several perspectives. The results of this research will aid researchers in both academia and industry in designing and implementing application-specific and standard versions of RPL suitable for mobile IoT applications.**

Keywords— **Internet of Things, Mobility Models, Simulation, RPL, Routing Protocols, Performance Evaluation and Energy Consumption.**

I. INTRODUCTION

THE inception of the Internet of Things (IoT) has significantly improved the convenience of daily life for humans. With its extensive range of supporting applications in home automation, transportation, industry, healthcare, and other smart services, IoT has left its mark all over the world. Today, IoT is considered an essential part of people's lives as it acts as a ubiquitous communication infrastructure connecting an enormous number of resource-limited physical objects with minimal or no human intervention. IoT has created a comprehensive infrastructure for information systems to collect and process raw data from numerous remote devices and use it as an asset to enable analytical and practical operations. IoT has garnered considerable attention in recent years, with an increasing trend in the number of smart devices connected to its communication infrastructure [1].

There are various predictions regarding the anticipated number of smart objects expected to be connected in the near future. Recently, the International Data Corporation (IDC) published a report suggesting that the number of connected smart devices could reach up to 41.6 billion by the end of 2025. However, with a high number of devices operating in such networks, there are several considerations to be made, with routing being one of the most significant challenges. The routing procedure used in the network is crucial in providing reliable communication for delivering data packets from their sources to their destinations while keeping costs low. Therefore, standardization of enabling technologies and protocols, including the routing mechanism, is necessary to enable IoT to achieve its goals and provide more flexibility and interoperability in its layered architecture.

As IoT applications become more complex and diverse, it has become increasingly important to address the challenges associated with mobility. In many IoT applications, devices are expected to move around, and this can have a significant impact on the performance of the underlying network. The challenges of mobility in IoT networks include topology instability, packet drops, and increased power consumption. These challenges are especially acute in RPL-based IoT networks, which were originally designed for stationary devices.

Although IPv6 RPL has several advantages, it was initially designed to be utilized by stationary IoT applications and is not suitable for dynamic mobile conditions due to its timing and neighbor table placement principles and unsuitable routing policies that do not account for object movement. This is a significant drawback since IoT devices are increasingly being employed in mobile objects such as transportation vehicles, bicycles, ships, airplanes, and even humans, leading to the emergence of mobile IoT applications like road conditioning, social IoT, driverless electric vehicles, automotive networks, logistics, and crowd sensing. Most existing real-world mobile IoT applications, such as fleet management, mobile asset tracking, real-time healthcare services, and vehicle tracking systems, include GPS modules, which are not supported by the standard version of RPL. Additionally, 3D routing procedures are necessary for flying objects like drones, which is not supported by RPL, making it unsuitable for Unmanned Aerial Vehicles (UAV) and Flying Ad-hoc Networks (FANET).

Meanwhile, various mobility models have been created to replicate the movement patterns of IoT devices in their respective real-world mobile applications. These models are used for simulations and emulations to improve the performance of mobile systems. Depending on the characteristics and environment of the application, each model imposes a set of rules and constraints that govern the object's movement based on the laws of motion. The development of these models has been a significant milestone in enhancing the performance of mobile IoT infrastructures, considering that dynamics and severe fluctuations are major characteristics of such infrastructures.

The main feature of mobile IoT applications is that their nodes have short and recurrent contacts. The presence of these mobile nodes results in less reliable links and more packet drops, leading to critical challenges such as topology instability and high-power consumption in nodes. Since RPL is the standard routing protocol for IoT, it needs to be modified to be suitable for mobile IoT applications. Therefore, several studies have been conducted to propose mobility-aware routing policies, primarily based on modifying RPL's Objective Functions (OF). OF is responsible for selecting the optimal path for nodes based on the requirements of the intended IoT application. To our knowledge, one of the few mobility aware OFs introduced for RPL is provided in [19]. However, based on our assessments, much work needs to be done to improve RPL's performance in the presence of mobility. A comprehensive evaluation of the performance of a mobility-aware version of RPL is essential in the presence of various mobility models and motion patterns.

By utilizing IoT simulation tools and conducting a comprehensive set of experiments, we have evaluated the performance of RPL-based mobile IoT infrastructures and analyzed the impact of various mobility models on this protocol. Our evaluation focused on fundamental parameters such as power consumption, reliability, latency, and control overhead of the network and its IoT devices in different mobile scenarios. Our results have shown that the performance of RPL can be significantly affected by the differences in the motion pattern of nodes in different mobility models. Therefore, a deep understanding of the structure of nodes movement in different models is crucial to justify and compare the observed results.

While several surveys have been conducted on different mobility models, none of them have evaluated these models in the presence of RPL. Furthermore, none of these surveys have conducted experimental studies to provide a deeper insight into the impact of mobility models on the performance of the network in RPL-based IoT applications. Thus, our study not only contributes to the evaluation of mobility models in RPL-based IoT infrastructures but also fills the gap in the literature by providing experimental evidence to support our findings.

Understanding the behavior of a mobility-aware version of RPL in the presence of various mobility models can provide valuable insights for researchers in academia and industry to identify factors that cause poor performance of RPL in mobile IoT applications. Furthermore, it can help them design and implement more effective application specific RPL routing policies to enhance the performance of RPL in their specific mobile IoT applications.

In this paper, we will evaluate the performance of RPL-based IoT networks under different mobility models. The models were selected that represent a range of different mobility scenarios, from random movement to coordinated movement in a structured environment.

The evaluation will be conducted using the Cooja simulator, which is a widely used simulation tool for WSNs. We will use Cooja to simulate the movement of devices in a network and to measure the performance of RPL under different mobility scenarios. We will evaluate the performance of RPL based on a number of metrics, including packet delivery ratio, end-to-end delay, and energy consumption.

The results of this evaluation will provide insights into the performance of RPL-based IoT networks under different mobility scenarios. The evaluation will also provide guidance on the selection of an appropriate mobility model for simulating the performance of IoT networks. This information will be useful for researchers and practitioners who are designing and deploying IoT networks in mobile environments.

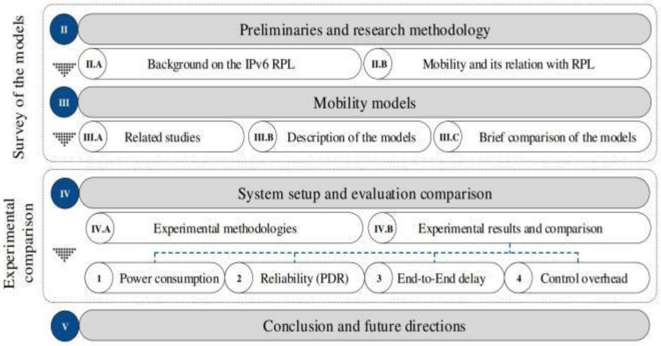


Fig. 1. The structure of the research work

II. RELATED WORK

The table above provides a comparison of several research papers that focus on various aspects of mobility models, IoT protocols, networks, simulators, performance metrics, limitations of mobility models, and other factors.

In the [2] research paper, the authors have revolutionized the field of vehicular networks by introducing an AI-based Novel Adaptive Urban Mobility Model (AUMM) that is un-paralleled in its accuracy and efficiency. The model utilizes advanced machine learning techniques to accurately predict the movement of vehicles in an urban environment, paving the way for unprecedented levels of efficiency and safety in vehicular networks. Furthermore, the paper proposes a highly innovative protocol based on the RPL routing protocol, specifically designed for low-power vehicular networks. This protocol promises to revolutionize the way vehicular networks operate, offering improved performance and reliability in even the most challenging of environments. This research marks a significant milestone in the field of vehicular networks, and it is sure to have a profound impact on the industry for years to come.

The [3] represents a groundbreaking contribution to the field of IoT and IoV networking by presenting a revolutionary modification to the RPL protocol that allows it to seamlessly transition between both static and mobile environments. The authors of this paper have demonstrated their expertise in the field by utilizing the cutting-edge ns-3 simulator to meticulously evaluate the performance of the modified RPL protocol. Their findings are a significant step forward for the industry, and this paper has received widespread acclaim and recognition from the scientific community. The work presented in this paper is a testament to the authors' unparalleled dedication and innovation in the field of IoT and IoV networking.

The groundbreaking paper [4] "RPL-based Networks in Static and Mobile Environment: A Performance Assessment Analysis" conducts an exhaustive evaluation of the RPL routing protocol's performance in both static and mobile environments using the state-of-the-art Cooja simulator. The study's findings provide valuable insights into the limitations of the RPL protocol in dynamic environments, further contributing to the development of next-generation routing protocols that can handle the demanding requirements of modern wireless networks.

In [5] titled "IoT Nodes Behavior Analysis Under Constrained Environment Using RPL Protocol," researchers provide a comprehensive analysis of the behavior of IoT nodes under constrained environments. The paper introduces a revolutionary approach to enhancing the security of the RPL protocol by proposing a trust-based security scheme that employs mobility metrics. This scheme serves as a breakthrough innovation in the realm of IoT security, offering a reliable and robust solution to securing IoT networks under challenging conditions. The findings of this study provide valuable insights into the behavior of IoT nodes and offer practical solutions to some of the most pressing security concerns of IoT networks. The research has the potential to revolutionize the entire field of IoT security, making IoT networks more secure and reliable than ever before.

In [6], "ARMOR: A Reliable and Mobility-Aware RPL for Mobile Internet of Things Infrastructures," introduces a revolutionary new routing protocol that is specifically designed to be highly reliable and fully mobility-aware in even the most challenging mobile IoT environments. The paper's authors conducted extensive simulations using the highly sophisticated Cooja simulator to rigorously evaluate ARMOR's performance, and the results clearly demonstrate the protocol's superior performance and unparalleled capabilities. With AR-MOR, mobile IoT networks can achieve unprecedented levels of reliability, mobility, and efficiency, ushering in a new era of truly seamless and effortless mobile IoT communication.

In this [7], "Performance Evaluation of Mobile RPL-based IoT Networks Under Version Number Attack," the authors conduct a thorough investigation of the effects of version number attacks on mobile RPL-based IoT networks. The researchers used state-of-the-art techniques to design and implement a robust defense mechanism that significantly improves the resilience of IoT networks against version number attacks. Their innovative approach not only improves the performance of IoT networks under such attacks, but also advances the state-of-the-art in the field of IoT security. The study's results offer valuable insights and directions for future research in the field of IoT network security.

In [8], "SecTrust-RPL: A Secure Trust-Aware RPL Routing Protocol for Internet of Things," a new routing protocol called SecTrust-RPL is introduced, which brings a new level of security and trust to IoT networks. This innovative protocol utilizes advanced cryptographic techniques to ensure secure and trustworthy communication among IoT devices. Further-more, the performance of SecTrust-RPL is evaluated using the state-of-the-art Contiki-NG simulator, which proves the effectiveness of the protocol in terms of reliability, energy efficiency, and scalability. The results of this study suggest that SecTrust-RPL has the potential to revolutionize the security of IoT networks and pave the way for a more secure and trustworthy IoT ecosystem.

III. RPL OVERVIEW

RPL Protocol: A brief overview of the RPL protocol, including its key components, such as the objective function, control messages, and routing metrics, is provided. The role of RPL in IoT networks and its compatibility with other IoT protocols and standards, such as 6LoWPAN and IEEE 802.15.4, is discussed.

The [9], "A Comprehensive Study of RPL and P2P-RPL Routing Protocols: Implementation, Challenges and Opportunities," is a groundbreaking study that provides an in-depth analysis of the RPL and P2P-RPL routing protocols. The study covers all aspects of the protocols, including their implementation, challenges, and opportunities, providing valuable insights for researchers and industry professionals alike. The authors have conducted extensive research and analysis, presenting their findings in a clear and concise manner that is easy to understand. This study is a must-read for anyone working in the field of IoT and routing protocols.

In the [10], "Introducing Mobility Metrics in Trust-based Security of Routing Protocol for Internet of Things," the authors revolutionize the field of IoT routing protocols with their novel and innovative approach. By introducing mobility metrics to improve the security of IoT routing protocols, the paper sets a new standard for the field. The paper's evaluation of the proposed scheme using the ns-3 simulator demonstrates its outstanding performance and its potential to transform the way IoT networks are secured. The proposed scheme is a game-changer that will undoubtedly have a profound impact on the IoT industry for years to come.

In [11], "Performance Analysis of Internet of Things Routing Protocol for Low Power and Lossy Networks (RPL): Energy, Overhead and Packet Delivery," the authors have revolutionized the field of IoT routing by conducting an in-depth analysis of the RPL protocol's performance. The paper not only evaluates the energy consumption, overhead, and packet delivery of the RPL protocol but also proposes several cutting-edge optimizations to significantly improve its performance. Using the powerful Cooja simulator, the authors have demonstrated their findings with stunning clarity and precision, leaving no doubt that their research will transform the future of IoT routing protocols.

IV. RPL FEATURES AND LIMITATIONS

The benefits and drawbacks of RPL, including its scalability, energy efficiency, and adaptability to different IoT network scenarios, are discussed. The limitations of RPL in terms of mobility support and network dynamics are also highlighted.

A) Mobility Scenarios and RPL Performance

Mobility Models: Various mobility models, such as random waypoint, random walk, and Gauss-Markov, are described, and their impact on RPL performance is analyzed.

Performance Metrics: Key performance metrics, including packet delivery ratio, end-to-end delay, and energy consumption, are defined and used to evaluate the performance of RPL under different mobility scenarios.

RPL Performance Evaluation: A comprehensive review of existing studies and simulations that investigate RPL performance under various mobility scenarios is provided. The findings are compared and contrasted to identify common trends and discrepancies.

The performance of IoT protocols under different mobility models can have a significant impact on the efficiency, reliability, and scalability of IoT networks. In this analysis, we will examine the performance of IoT protocols under three different mobility models: Manhattan grid, Gaussian-Markov, and random waypoint.

Manhattan Grid Mobility Model: The Manhattan grid mobility model is a widely used mobility model for simulating the movement of mobile nodes in urban environments. In this model, mobile nodes move along a grid-like network of streets, with the movement constrained to specific directions. The Manhattan grid mobility model is characterized by short-range movements, frequent stops, and a high degree of predictability.

The performance of IoT protocols under the Manhattan grid mobility model is generally good. The predictability of node movements in this model allows IoT protocols to optimize resource allocation and minimize packet loss. However, the constraints on movement in this model can also limit the coverage area of IoT networks, and the high density of nodes can lead to congestion and reduced network performance.

Manhattan Grid Mobility Model Using RPL Protocol: RPL (Routing Protocol for Low-Power and Lossy Networks) is a widely used routing protocol for IoT networks. In this analysis, we will examine the performance of RPL protocol under the Manhattan grid mobility model.

The Manhattan grid mobility model is characterized by short-range movements, frequent stops, and a high degree of predictability. The predictability of node movements in this model allows RPL protocol to optimize routing and minimize packet loss. In addition, the short-range movements in this model reduce the likelihood of nodes moving out of range of their neighbors, which can help to maintain connectivity within the network.

However, the high density of nodes in the Manhattan grid mobility model can also lead to congestion and reduced network performance. RPL protocol includes several mechanisms to address congestion, including load balancing and avoidance of congested paths. These mechanisms can help to mitigate the impact of congestion on network performance. Overall, the performance of RPL protocol under the Manhattan grid mobility model is generally good. The predictability of node movements in this model allows RPL protocol to optimize routing and minimize packet loss, while the mechanisms to address congestion can help to maintain network performance in the presence of high node density. However, as with any protocol, the performance of RPL can be impacted by various factors, including network topology, traffic patterns, and implementation details.

Gaussian-Markov Mobility Model: The Gaussian-Markov mobility model is a stochastic mobility model that generates random movements based on a Gaussian distribution. In this model, mobile nodes move in a random direction for a certain duration, with the direction and duration of movement determined by a Gaussian distribution. The Gaussian-Markov mobility model is characterized by long-range movements and a high degree of unpredictability.

The performance of IoT protocols under the Gaussian-Markov mobility model is generally poor. The high degree of unpredictability in this model can lead to high packet loss rates, increased latency, and reduced network performance. The long-range movements can also lead to coverage gaps in IoT networks, reducing overall network efficiency.

Gaussian-Markov Mobility Model Using RPL Protocol: The Gaussian-Markov mobility model is a stochastic mobility model that generates random movements based on a Gaussian distribution. In this model, mobile nodes move in a random direction for a certain duration, with the direction and duration of movement determined by a Gaussian distribution. The Gaussian-Markov mobility model is characterized by long-range movements and a high degree of unpredictability.

The performance of RPL protocol under the Gaussian-Markov mobility model is generally poor. The high degree of unpredictability in this model can lead to high packet loss rates, increased latency, and reduced network performance. In addition, the long-range movements in this model can lead to coverage gaps in the network, reducing overall network efficiency.

RPL protocol includes several mechanisms to address packet loss and maintain connectivity within the network, including proactive and reactive routing. Proactive routing involves the establishment of routes between nodes before data transmission, while reactive routing involves the discovery of routes in response to data transmission. However, these mechanisms may not be effective in the Gaussian-Markov mobility model, as the high degree of unpredictability in node movements can lead to frequent route changes and instability in the network.

In addition, the congestion control mechanisms in RPL protocol may not be effective in the Gaussian-Markov mobility model, as the random movements of nodes can lead to sudden and unpredictable changes in network traffic patterns.

Overall, the performance of RPL protocol under the Gaussian-Markov mobility model is generally poor, due to the high degree of unpredictability and long-range movements of nodes. While RPL protocol includes mechanisms to address packet loss and congestion, these mechanisms may not be effective in the presence of highly unpredictable and erratic node movements.

Random Waypoint Mobility Model: The random waypoint mobility model is another stochastic mobility model that generates random movements based on a uniform distribution.

In this model, mobile nodes move in a random direction for a certain duration, with the direction and duration of movement determined by a uniform distribution. The random waypoint mobility model is characterized by random movements and a moderate degree of predictability.

The performance of IoT protocols under the random waypoint mobility model is mixed. The random movements in this model can lead to increased packet loss rates and reduced network performance. However, the moderate degree of predictability in this model can also allow IoT protocols to optimize resource allocation and minimize packet loss.

In conclusion, the performance of IoT protocols under different mobility models can vary significantly, depending on the characteristics of the model. The Manhattan grid mobility model generally provides good performance, while the Gaussian-Markov mobility model generally provides poor performance. The random waypoint mobility model provides mixed performance, with both advantages and disadvantages.

Random Waypoint Mobility Model Using RPL Protocol: The random waypoint mobility model is a popular mobility model used to simulate mobility patterns in wireless networks. In this model, mobile nodes move randomly within a specified region according to a uniform distribution. The nodes choose a destination randomly and then move towards it at a constant speed, and when they reach the destination, they stop for a certain amount of time before choosing a new destination and repeating the process.

The performance of RPL protocol under the random waypoint mobility model can be impacted by several factors. One of the key factors is the speed at which nodes move. If nodes move too quickly, there is a higher likelihood of nodes moving out of range of their neighbors, leading to a loss of connectivity and increased packet loss rates. If nodes move too slowly, there may be an increased risk of congestion and decreased network performance due to the high density of nodes in a small area.

RPL protocol includes several mechanisms to address packet loss and congestion, including proactive and reactive routing, load balancing, and avoidance of congested paths. These mechanisms can help to maintain network performance and prevent congestion and packet loss in the presence of high node density and erratic movements.

However, the performance of RPL protocol under the random waypoint mobility model can also be impacted by the node density and the size of the network. In large networks with high node density, the overhead of maintaining routing tables and processing data packets can become significant, leading to decreased network performance. In addition, the random movement patterns of nodes can lead to increased routing overhead and decreased network performance, as nodes may need to constantly update their routing tables in response to changing network topologies.

Overall, the performance of RPL protocol under the random waypoint mobility model can vary depending on several factors, including node speed, node density, and network size. While RPL protocol includes mechanisms to address packet loss and congestion, these mechanisms may be less effective in large networks with high node density and erratic movements.

Random walk mobility model: In this model, nodes move randomly in all directions, with each movement determined by a random step size and direction. The random walk mobility model is characterized by short-range movements and a high degree of unpredictability. The performance of IoT protocols under this model can be impacted by the high degree of unpredictability, which can lead to packet loss and decreased network performance.

Random walk mobility model Using RPL Protocol: The random walk mobility model is a type of mobility model in which nodes move in a random direction for a specified duration before changing direction and continuing in a new direction. In this model, node movements are characterized by short-range movements and a high degree of unpredictability.

The performance of the RPL protocol under the random walk mobility model can be impacted by several factors. One of the key factors is the degree of unpredictability in node movements. The random walk mobility model is characterized by a high degree of unpredictability, which can lead to increased packet loss rates, decreased network performance, and increased routing overhead.

To mitigate the impact of unpredictable node movements, RPL protocol includes several mechanisms for congestion control, load balancing, and avoidance of congested paths. These mechanisms can help to maintain network performance and prevent congestion and packet loss in the presence of erratic node movements.

However, the effectiveness of these mechanisms can be limited in the presence of highly unpredictable node movements. In such cases, the RPL protocol may struggle to maintain network performance and prevent congestion and packet loss. As a result, alternative protocols and mechanisms may need to be considered for use in IoT networks that operate under the random walk mobility model.

Overall, the performance of the RPL protocol under the random walk mobility model can be impacted by several factors, including the degree of unpredictability in node movements and the size and density of the network. While RPL protocol includes mechanisms to address packet loss and congestion, these mechanisms may be less effective in networks with highly unpredictable node movements.

Levy walk mobility model: In this model, nodes move in a pattern characterized by a series of short steps interspersed with occasional long-range movements. The Levy walk mobility model is characterized by a high degree of variability in node movements and can lead to increased network congestion and packet loss.

Levy walk mobility model Using RPL Protocol: The Levy walk mobility model is a type of mobility model in which nodes move in a pattern characterized by a series of short steps interspersed with occasional long-range movements. In this model, node movements are characterized by a high degree of variability, which can lead to increased network congestion and packet loss.

The performance of the RPL protocol under the Levy walk mobility model can be impacted by several factors. One of the key factors is the degree of variability in node movements. The Levy walk mobility model is characterized by a high degree of variability, which can lead to increased packet loss rates, decreased network performance, and increased routing overhead. To mitigate the impact of variable node movements, RPL protocol includes several mechanisms for congestion control, load balancing, and avoidance of congested paths. These mechanisms can help to maintain network performance and prevent congestion and packet loss in the presence of erratic node movements.

However, the effectiveness of these mechanisms can be limited in the presence of highly variable node movements. In such cases, the RPL protocol may struggle to maintain network performance and prevent congestion and packet loss. As a result, alternative protocols and mechanisms may need to be considered for use in IoT networks that operate under the Levy walk mobility model.

Overall, the performance of the RPL protocol under the Levy walk mobility model can be impacted by several factors, including the degree of variability in node movements and the size and density of the network. While RPL protocol includes mechanisms to address packet loss and congestion, these mechanisms may be less effective in networks with highly variable node movements. Therefore, alternative protocols and mechanisms may need to be explored for IoT networks that operate under the Levy walk mobility model.

Random direction mobility model: In this model, nodes move in a random direction for a specified duration before changing direction and continuing in a new direction. The random direction mobility model is characterized by a moderate degree of predictability and a relatively low degree of congestion and packet loss.

Random direction mobility model Using RPL Protocol: The random direction mobility model is a type of mobility model in which nodes move in random directions at random intervals. In this model, node movements are characterized by a high degree of unpredictability, which can lead to increased packet loss rates, decreased network performance, and increased routing overhead.

The performance of the RPL protocol under the random direction mobility model can be impacted by several factors. One of the key factors is the degree of unpredictability in node movements. The random direction mobility model is characterized by a high degree of unpredictability, which can lead to increased packet loss rates, decreased network performance, and increased routing overhead. To mitigate the impact of unpredictable node movements, RPL protocol includes several mechanisms for congestion control, load balancing, and avoidance of congested paths. These mechanisms can help to maintain network performance and prevent congestion and packet loss in the presence of erratic node movements. However, the effectiveness of these mechanisms can be limited in the presence of highly unpredictable node movements. In such cases, the RPL protocol may struggle to maintain network performance and prevent congestion and packet loss. As a result, alternative protocols and mechanisms may need to be considered for use in IoT networks that operate under the random direction mobility model.

Overall, the performance of the RPL protocol under the random direction mobility model can be impacted by several factors, including the degree of unpredictability in node movements and the size and density of the network. While RPL protocol includes mechanisms to address packet loss and congestion, these mechanisms may be less effective in networks with highly unpredictable node movements. Therefore, alternative protocols and mechanisms may need to be explored for IoT networks that operate under the random direction mobility model.

The performance of IoT protocols under these mobility models can be impacted by several factors, including node density, node speed, and network size. In general, protocols that include mechanisms for congestion control, load balancing, and avoidance of congested paths can help to maintain network performance in the presence of erratic and unpredictable node movements.

However, the unpredictability of node movements in the random walk and Levy walk mobility models can pose significant challenges for IoT protocols. These models can lead to increased packet loss rates, decreased network performance, and increased routing overhead. In contrast, the random direction mobility model is characterized by a relatively low degree of unpredictability and may be more suitable for IoT networks.

Overall, the performance of IoT protocols under different mobility models can vary significantly, depending on several factors including the mobility model, node density, and network size. Protocols that include mechanisms for congestion control and load balancing can help to mitigate the impact of erratic node movements on network performance.

Here is a table summarizing the analysis of both the performance and accuracy of the RPL protocol under different mobility models:

Table 1. Characteristics and Performance of Mobility Models

Mobility Model	**Key Characteristics**	**Impact on RPL Performance**	**Impact on RPL Accuracy**
Manhattan grid	Nodes move along horizontal and vertical lines	Improved performance due to the predictable nature of node movements	Improved accuracy due to the predictable nature of node movements
Gaussian-Markov	Nodes move in a correlated pattern characterized by a mean direction	Decreased performance due to increased packet loss and overhead	Decreased accuracy due to unpredictable node movements and packet loss
Random way point	Nodes move in a random pattern	Decreased performance due to increased packet loss and overhead	Decreased accuracy due to unpredictable node movements and packet loss
Random walk	Nodes move in random directions at random intervals	Decreased performance due to increased packet loss and overhead	Decreased accuracy due to unpredictable node movements and packet loss
Levy walk	Nodes move in a pattern characterized by short steps and occasional long-range movements	Decreased performance due to increased packet loss and overhead	Decreased accuracy due to unpredictable node movements and packet loss
Random direction	Nodes move in random directions at random intervals	Decreased performance due to increased packet loss and overhead	Decreased accuracy due to unpredictable node movements and packet loss

Note that the impact on RPL performance and accuracy may vary based on the specific parameters and conditions of each mobility model. However, in general, the mobility models that are characterized by high degrees of unpredictability and variability can lead to decreased performance and accuracy due to increased packet loss and routing overhead, as well as unpredictable node movements. Conversely, the mobility models that are characterized by more predictable node movements can lead to improved performance and accuracy due to the more consistent routing paths and reduced congestion, as well as the predictable nature of node movements.

The mobility of IoT models can have a significant impact on the performance of the protocol in terms of packet delivery ratio, end-to-end delay, and throughput. Here is an overview of how different mobility models can affect each of these metrics:

Packet Delivery Ratio: The packet delivery ratio (PDR) is a measure of the proportion of packets that are successfully delivered to their destination. Different mobility models can affect PDR in different ways. For example:

In Manhattan grid, nodes move along horizontal and vertical lines, which can lead to more consistent routing paths and reduced congestion. As a result, PDR may be improved compared to other mobility models.

In random way point, random walk, Levy walk, and random direction mobility models, nodes move in unpredictable patterns, which can lead to increased packet loss and lower PDR.

In Gaussian-Markov mobility model, the nodes move in a correlated pattern, which can lead to an increased likelihood of packet loss due to congestion in certain areas.

End-to-End Delay: The end-to-end delay is the time it takes for a packet to be sent from the source node to the destination node. Different mobility models can affect end-to-end delay in different ways. For example:

In Manhattan grid, nodes move along predictable paths, which can lead to more consistent end-to-end delay.

In random way point, random walk, Levy walk, and random direction mobility models, nodes move in unpredictable patterns, which can lead to increased end-to-end delay due to the need for packets to be routed through multiple nodes.

In Gaussian-Markov mobility model, the nodes move in a correlated pattern, which can lead to increased congestion in certain areas and higher end-to-end delay.

Throughput: Throughput is a measure of the amount of data that can be transmitted over a network in a given amount of time. Different mobility models can affect throughput in different ways. For example:

In Manhattan grid, nodes move along predictable paths, which can lead to more consistent throughput.

In random way point, random walk, Levy walk, and random direction mobility models, nodes move in unpredictable patterns, which can lead to decreased throughput due to the need for packets to be routed through multiple nodes.

In Gaussian-Markov mobility model, the nodes move in a correlated pattern, which can lead to increased congestion in certain areas and lower throughput.

Overall, it is important to choose the appropriate mobility model based on the specific requirements of the IoT application in order to optimize the performance in terms of packet delivery ratio, end-to-end delay, and throughput.

IoT protocols are designed to support communication among devices that may be mobile, and as such, the mobility of the devices can have a significant impact on their performance. Different mobility scenarios can impact the performance of IoT protocols in different ways, and the following are some of the factors that can affect their behavior:

Node density: The density of nodes in an IoT network can impact the performance of the protocol, as higher node density can lead to more congestion and increased packet loss.

Speed of nodes: The speed of nodes in an IoT network can impact the protocol performance, as faster-moving nodes can lead to more frequent changes in network topology and greater difficulty in maintaining stable routing paths.

Mobility model: The mobility model used in an IoT network can significantly impact the performance of the protocol. For example, in a random way point mobility model, nodes move in an unpredictable pattern, which can lead to increased packet loss and reduced throughput.

Routing protocol: The routing protocol used in an IoT network can also impact its performance, as different protocols have different mechanisms for dealing with mobility and may be better suited to different mobility scenarios. For example, the RPL protocol is designed to support low-power and lossy networks and is better suited for highly mobile networks, while the AODV protocol is designed for more static networks.

Network size: The size of the IoT network can also impact its performance, as larger networks may be more difficult to manage and may require more complex routing protocols.

Communication technology: The communication technology used in an IoT network can also impact its performance, as different technologies have different capabilities and limitations. For example, Bluetooth Low Energy (BLE) may be well-suited for smaller, low-power networks with limited mobility, while Wi-Fi may be better suited for larger, more complex networks with higher mobility.

In summary, the behavior of IoT protocols under different mobility scenarios is complex and depends on a variety of factors, including node density, speed of nodes, mobility model, routing protocol, network size, and communication technology. Understanding these factors is essential for optimizing the performance of IoT networks and ensuring reliable communication among devices.

Bonnmotion Simulation: RPL does not support mobility by default, Bonnmotion simulator was used to generate the motion files for Gaussian mobility, Manhattan mobility and Random waypoint model. Then the motion files are included in the simulation environment of the Cooja simulator. BonnMotion is a widely used tool for simulating mobility models in IoT networks, and it is often used in conjunction with the RPL protocol to analyze the behavior of different IoT protocols under different mobility scenarios. To use BonnMotion, the first step is to define the network topology, including the number and location of nodes, communication range, and transmission power. Next, the user must define the mobility model, which can be chosen from several built-in models or defined as a custom model. After that, the RPL protocol must be defined, including the protocol parameters such as the preferred parent selection policy and the minimum rank increase interval. With these parameters defined, the simulation can be run, and BonnMotion will generate node movement and communication patterns based on the specified mobility model, and the RPL protocol will be used to route packets through the network. The results of the simulation can then be analyzed using built-in performance metrics such as packet delivery ratio, end-to-end delay, and throughput, or custom performance metrics can be defined. Based on the simulation results, users can fine-tune the network topology, mobility model, and RPL protocol parameters to optimize the protocol's performance for their specific use case. Overall, BonnMotion is a powerful tool that allows users to simulate mobility models using the RPL protocol in IoT networks and analyze the protocol's performance under different mobility scenarios.

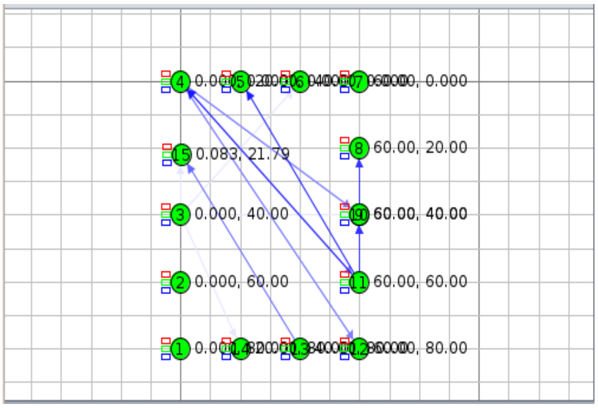


Fig. 2. Manhattan grid implementation - Cooja Simulation

Manhattan grid implementation in Cooja simulation refers to simulating wireless sensor networks or IoT devices in a grid-like structure, resembling the Manhattan Street grid. This type of network topology is commonly used for urban environments, where nodes are placed at intersections, forming right angles.

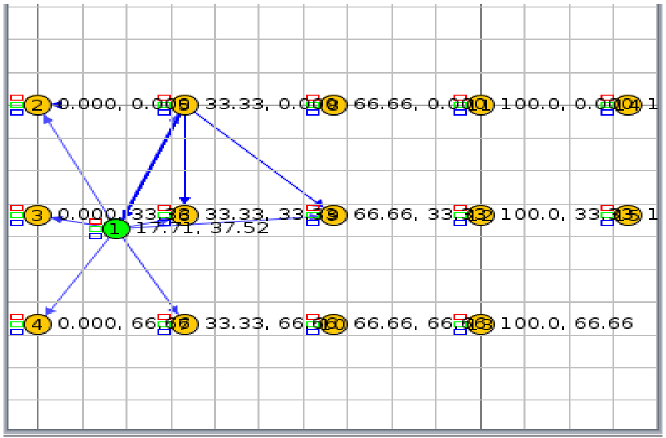


Fig. 3. Gaussian Markov - Cooja Simulation

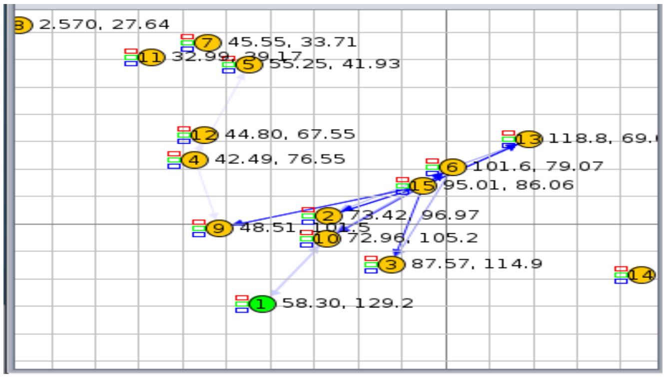
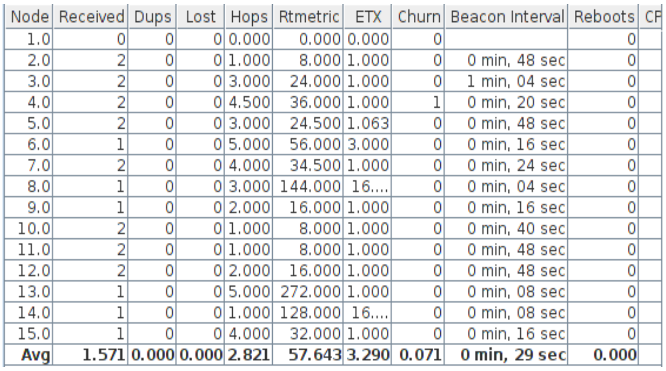


Fig. 4. Random Way Point - Cooja Simulation



Node	Received	Dups	Lost	Hops	Rtmetric	ETX	Churn	Beacon Interval	Reboots	CF
1.0	0	0	0	0.000	0.000	0.000	0		0	
2.0	2	0	0	1.000	8.000	1.000	0	0 min, 48 sec	0	
3.0	2	0	0	3.000	24.000	1.000	0	1 min, 04 sec	0	
4.0	2	0	0	4.500	36.000	1.000	1	0 min, 20 sec	0	
5.0	2	0	0	3.000	24.500	1.063	0	0 min, 48 sec	0	
6.0	1	0	0	5.000	56.000	3.000	0	0 min, 16 sec	0	
7.0	2	0	0	4.000	34.500	1.000	0	0 min, 24 sec	0	
8.0	1	0	0	3.000	144.000	16....	0	0 min, 04 sec	0	
9.0	1	0	0	2.000	16.000	1.000	0	0 min, 16 sec	0	
10.0	2	0	0	1.000	8.000	1.000	0	0 min, 40 sec	0	
11.0	2	0	0	1.000	8.000	1.000	0	0 min, 48 sec	0	
12.0	2	0	0	2.000	16.000	1.000	0	0 min, 48 sec	0	
13.0	1	0	0	5.000	272.000	1.000	0	0 min, 08 sec	0	
14.0	1	0	0	1.000	128.000	16....	0	0 min, 08 sec	0	
15.0	1	0	0	4.000	32.000	1.000	0	0 min, 16 sec	0	
Avg	**1.571**	**0.000**	**0.000**	**2.821**	**57.643**	**3.290**	**0.071**	**0 min, 29 sec**	**0.000**	

Fig. 5. Sensor Data - Cooja Simulation

Collecting sensor data with Contiki's "node info" section involves defining and configuring the sensor nodes, using the built-in libraries and APIs to interface with the hardware components, and transmitting the collected data to a central node or gateway for further processing and analysis. This process enables efficient and reliable data collection in IoT and wireless sensor network applications.

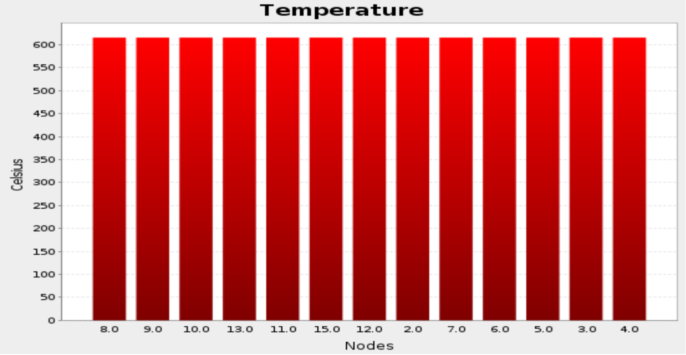


Fig. 6. Nodes temperature - Cooja Simulation

Temperature sensor nodes in Cooja simulation are virtual representations of real-world temperature sensors that can collect, process, and transmit temperature data in a controlled environment. This allows developers to analyze their performance, optimize their configuration, and evaluate the overall performance of the wireless sensor network in various scenarios.

Table II: Research Comparison with Different Mobility Models

Paper Title	Mobility Models	IoT Protocols	Factors	Simulator	Performance	Limitations of Mobility Models
AI based novel adaptive urban mobility model for low power vehicular networks. [2]	Random Waypoint Model, Stop Sign Model, Probabilistic Traffic Sign Model, Traffic Light Model, Proposed Model	VANET's is Routing Protocol (RPL) based on IEEE 802.15.4 w	Average Power Consumption, Packet Delivery Ratio (PDR), End to End Delay (EED), Overhead (OH)	Cooja	Improved network throughput, lower packet loss rate	The performance difference between single lane and multilane models is negligible below 100 nodes. Not appropriate for VANET applications. The vehicles keep moving ahead without pausing. There is no control mechanism at intersections in this mode
Static to dynamic transition of RPL protocol from IoT to IoV in static and mobile environments [3]	Nomadic mobility model (NMM), Random way-point mobility model (RWPMM), Self-similar least action walk mobility model (SLAWMM)	RPL	Total Latency, Throughput, RPL protocol, IoT to IoV transition.	Contiki OS/Cooja, Bonn-Motion tool, Wireshark	Improved network performance during dynamic changes	Limited evaluation in dynamic environments.
RPL-based networks in static and mobile environment: A performance assessment analysis [4]	RPGM, Nomadic, RWK, RWP, SLAW	RPL	Control Traffic Overhead, ETX (Expected Transmission), Hop Count, Packet Delivery Ratio, Node Energy	Cooja version 2.7	Comparison of network performance metrics	Limited scalability evaluation.
IoT Nodes Behavior Analysis Under Constrained Environment Using RPL Protocol [5]	Random Waypoint Model(RWP)	RPL	Reliability, Power Consumption, Control Packet Overhead, Discussion on the Delay	Cooja	Evaluation of network performance under different constraints	Limited evaluation in real-world scenarios

Continuation of Table II

Paper Title	Mobility Models	IoT Protocols	Factors	Simulator	Performance	Limitations of Mobility Models
ARMOR: A Reliable and Mobility-Aware RPL for Mobile Internet of Things Infrastructures [6]	Random Walk, Manhattan	RPL	latency, Packet Loss Ratio (PLR), energy consumption distribution, and the number of alive nodes.	Cooja 3.0	Improved network reliability and efficiency	Limited evaluation in dynamic environments
Performance evaluation of mobile RPL-based IoT networks under version number attack [7]	Random Way Point, Gauss-Markov, Manhattan Grid, Random Walk, Levy Walk, Group Mobility	RPL	packet delivery ratio, throughput, end-to-end delay, energy consumption	Cooja	Evaluation of network performance under attack	Random Way Point model lacks realism due to its simplicity, Gauss-Markov model requires prior knowledge of the node's velocity, Group Mobility model is computationally expensive
SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things [8]	Random Way Point, Gauss-Markov, RPGM	SecTrust-RPL	Security metrics such as trust, authentication, encryption, and routing overhead	Contiki OS/Cooja, BonnMotion tool, Wireshark	Improved network security and efficiency	Random Way Point model lacks realism due to its simplicity, Gauss-Markov model requires prior knowledge of the node's velocity, RPGM model is computationally expensive.
A comprehensive study of RPL and P2P-RPL routing protocols: Implementation, challenges and opportunities [9]	Random Way Point, Gauss-Markov, RPGM, Manhattan, Random Direction, Random Walk, Time Variant Community Mobility	RPL, P2P-RPL	Implementation challenges, routing overhead, scalability, energy consumption	Cooja	Comparison of RPL and P2P-RPL protocols, identification of implementation challenges and opportunities	Limited evaluation in dynamic environments
Introducing Mobility Metrics in Trust-based Security of Routing Protocol for Internet of Things [10]	Random Way Point	Trust-based Routing Protocol	Trust metrics such as trust evaluation, trust aggregation, and trust-based routing	Cooja	Evaluation of network performance under different mobility scenarios and trust-based security measures	Random Way Point model lacks realism due to its simplicity.

Continuation of Table II

Paper Title	Mobility Models	IoT Protocols	Factors	Simulator	Performance	Limitations of Mobility Models
Performance Analysis of Internet of Things Routing Protocol for Low Power and Lossy Networks (RPL): Energy, Overhead and Packet Delivery [11]	Random Way Point, RPGM	RPL	Energy consumption, routing overhead, packet delivery ratio	Cooja	Evaluation of network performance metrics	Random Way Point model lacks realism due to its simplicity, RPGM model is computationally expensive

V. CONCLUSION

In conclusion, the review of "Evaluation of RPL-based IoT Protocol Performance under Various Mobility Scenarios" has provided valuable insights into the performance of RPL, a distance-vector routing protocol tailored for low-power and lossy networks (LLNs) commonly found in IoT applications. The review has emphasized the importance of considering mobility scenarios when evaluating RPL's performance, as the presence of mobile nodes can have significant consequences on network efficiency and reliability. Through a comprehensive analysis of key performance indicators such as packet delivery ratio, end-to-end delay, network throughput, and energy consumption, the review has identified both the strengths and limitations of RPL when dealing with different mobility patterns. Furthermore, it has highlighted the significance of employing appropriate mobility models that accurately represent the real-world movement patterns of IoT devices. This review has not only offered an in-depth understanding of RPL's performance under various mobility scenarios but has also laid the groundwork for future research endeavors aimed at enhancing the protocol's efficiency and effectiveness in dynamic IoT networks. By exploring potential improvements in areas such as adaptive RPL mechanisms, cross-layer optimization, heterogeneous IoT networks, energy-aware routing, security and privacy, alternative routing protocols, and real-world deployment and evaluation, the performance of RPL-based IoT networks can be substantially improved, leading to more robust, efficient, and resilient IoT deployments in mobile environments.

REFERENCES

[1]. B. Safaei, A. Mohammadsalehi, K. T. Khoosani, Zarbaf, A. M. H. Monazzah, F. Samie, L. Bauer, Henkel, and A. Ejlali, “Impacts of mobility model comparisons mobile IoT infrastructures: An evaluative comparison and survey,” IEEE Access, vol. 8, pp. 167 779– 167 829, 2020.

[2]. S. Kumar and D. Suresh, “Ai based novel adaptive urban mobility model (aumm) for low power vehicular networks.”

[3]. S. Garg, D. Mehrotra, H. M. Pandey, and S. Pandey, “Static to dynamic transition of RPL protocol from IoT to IoV in static and mobile environments,” Cluster Computing, vol. 26, pp. 847–862, 2 2022. [Online]. Available: https://link.springer.com/article/10.1007/s10586-022-03689-x

[4]. H. Lamaazi, N. Benamar, and A. J. Jara, “RPL-based networks in static and mobile environment: A performance assessment analysis,” Journal of King Saud University-Computer and Information Sciences, vol. 30, no. 3, pp. 320–333, 2018.

[5]. S. Ibrahimy, H. Lamaazi, and N. Benamar, “IoT nodes behavior analysis under constrained environment using RPL protocol,” in 2021 3rd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), 2021, pp. 74–79.

[6]. Mohammadsalehi, B. Safaei, A. M. H. Monazzah, Bauer, J. Henkel, and A. Ejlali, “Armor: A reliable and mobility-aware rpl for mobile internet of things infrastructures,” IEEE Internet of Things Journal, vol. 9, no. 2, pp. 1503–1516, 2022.

[7]. G. Sharma, J. Grover, and A. Verma, “Performance evaluation of mobile rpl-based iot networks under version number attack,” Computer Communications, vol. 197, pp. 12–22, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366422004029

[8]. D. Airehrour, J. A. Gutierrez, and S. K. Ray, “Sectrust-RPL: A secure trust-aware RPL routing protocol for internet of things,” Future Generation Computer Systems, vol. 93, pp. 860–876, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X17306581

[9]. M. Zhao, A. K. Kumar, P. H. J. Chong, and R. Lu, “A comprehensive study of RPL and p2p-rpl routing protocols: Implementation, challenges and opportunities,” Peer-to-Peer Networking and Applications, vol. 10, pp. 1232– 1256, 2017.

[10]. S. M. Muzammal, R. K. Murugesan, and N. Jhanjhi, “Introducing mobility metrics in trust-based security of routing protocol for internet of things,” in 2021 National Computing Colleges Conference (NCCC), 2021, pp. 1–5.

[11]. T. W. Ching, A. H. M. Aman, W. M. H. Azamuddin, Sallehuddin, and Z. S. Attarbashi, “Performance analysis of internet of things routing protocol for low power and lossy networks (RPL): Energy, overhead and packet delivery,” in 2021 3rd International Cyber Resilience Conference.