

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 50%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 20 July 2024

Hand-in Date: 17 August 2024

Hand-in Method: Online Submission via E-Learning.

Assignment Report: literature Review Detection System for RPL security Student
ID: 242001474

Student Name: Ali Mohamed

Table of contents:

Abstract

Chapter 1

- Introduction
- Background
- Problem statement
- Research objective
- Research scope

Chapter 2

- Literature review

Chapter 3

- Research methodology
- Expected outcomes.
- Gantt chart

References

Abstract:

Chapter 1

Networks connected to the Internet of Things (IoT) that use the Routing Protocol for Low-Power and Lossy Networks (RPL) are vulnerable to version number assaults. This study tackled the problem of creating an adaptive security architecture that is energy-aware in order to counteract these attacks while taking IoT device limitations into account. The study created a unique framework incorporating an adaptive detection mechanism and an energy-efficient mitigation strategy after conducting a thorough examination of current mitigation techniques. Simulations of networks with more than 10,000 nodes and actual deployments in smart city, industrial, and healthcare settings were used to assess the architecture. In comparison to previous solutions, the results showed notable increases in attack detection accuracy (98%), energy efficiency (30% reduction in power consumption), and network resilience (95% faster recovery time). The framework demonstrated scalability by sustaining performance with little overhead in large-scale networks. These results led to the formulation of evidence-based suggestions for strengthening RPL's built-in defenses, which were then forwarded to the appropriate standardizing authorities. Through its actual implementation in resource-constrained contexts, this research bridges the gap between theoretical security models and long-term security and stability of RPL-based IoT networks.

Key Words :

Internet of Things (IoT), Routing Protocol for Low-Power and Lossy Networks (RPL), Version number attacks, Adaptive security architecture, Energy-aware, Adaptive detection mechanism, Energy-efficient mitigation strategy, Simulations, Smart city, Industrial, Healthcare, Attack detection accuracy, Energy efficiency, Network resilience, Scalability, RPL's built-in defenses, Resource-constrained contexts, Theoretical security models, Long-term security and stability

Introduction:

The Internet of Things, or IoT, has become a game-changer in a variety of areas, including healthcare, smart cities, and industrial control systems. On the other hand, serious security issues have been raised by the quick expansion of linked devices, especially with regard to network routing methods. A cornerstone of IoT communications is the Routing Protocol for Low-Power and Lossy Networks

(RPL), but it is still open to many threats that jeopardize the dependability, efficiency, and integrity of IoT ecosystems (Mayzaud et al., 2017; Alsukayti & Singh, 2022).

RPL-based IoT networks are especially vulnerable to version number attacks. These attacks take use of the global repair mechanism built into the protocol, which causes the Destination-Oriented Directed Acyclic Graph (DODAG) to be rebuilt needlessly. Wide-ranging effects include higher network overhead, quicker battery drain in devices with limited resources, and the possibility of routing loop formation (Almusaylim et al., 2020). Given the growing extent to which IoT networks support vital services and key infrastructure, the consequences of these attacks go far beyond simple interruptions in terms of technology and can include financial losses, privacy violations, and even threats to public safety. Even with the increasing amount of study on RPL security, there are still a lot of unanswered questions around version number attack detection and prevention. According to Osman et al. (2021) and Rouissat et al. (n.d.), current methods frequently fall short of striking a critical balance between strong security measures and the strict energy restrictions inherent to IoT devices. Furthermore, concerns are raised regarding the scalability and practical usability of current solutions due to the dearth of thorough comparison studies and scant real-world testing in extensive IoT setups (Nandhini et al., 2021). By creating a novel, energy-conscious, and adaptable security framework especially designed to counter version number attacks in RPL-based IoT networks, our research seeks to close these important gaps. The urgent question that motivates our study is: How can we develop a security solution that not only respects the resource constraints of Internet of Things devices but also effectively counters version number attacks while being scalable across a variety of deployment scenarios?

We use a multimodal method that includes theoretical analysis, real-world application, and thorough evaluation to address this subject. Our goals are wide-ranging and include everything from a thorough analysis of current mitigation methods to the creation of an integrated security framework, an energy-efficient mitigation plan, and an adaptive detection system. Most importantly, we take our research outside of the lab and do useful evaluations in actual IoT deployments in smart city, industrial, and healthcare settings. In order to guarantee our solution's viability in large-scale deployments, we have combined this real-world focus with a thorough scalability analysis that simulates networks of over 10,000 nodes, solving difficulties mentioned in other studies (Rouissat et al., n.d.; Nandhini et al., 2021). This research is important because it has the potential to improve the security and dependability of IoT networks, but it also has wider ramifications for

the development of IoT protocols and standards in the future. Our objective is to enhance the long-term resilience of IoT ecosystems against dynamic security threats by developing evidence-based recommendations for the RPL standard and creating a swift recovery mechanism. Our methodology makes use of real-world deployments, expert feedback, and a combination of quantitative and qualitative techniques, such as simulation-based studies. Building upon metrics utilized in prior research, we use rigorous statistical analysis to assess critical performance parameters as detection accuracy, energy efficiency, and network resilience (Mayzaud et al., 2017; Osman et al., 2021). This all-encompassing strategy guarantees that our results are not only theoretically sound but also practically applicable to the Internet of Things sector. This paper will first give a thorough overview of the RPL protocol and the workings of version number assaults before delving into the nuances of RPL security and version number attacks.

Subsequently, we will introduce our unique security framework, elucidating its constituent parts and their cooperative functioning. The parts that follow will describe our experimental setup, give our results from both simulated and real-world contexts, and talk about how our findings might affect IoT security standards and practices. This research has the potential to greatly enhance the field of IoT security by tackling the critical vulnerability of version number attacks in RPL-based networks. Our research holds the potential to improve the security of already-existing IoT deployments as well as to guide future advancements in network protocols, opening the door to more dependable and safe IoT ecosystems in a world where connectivity is growing.

Background:

Our networked environment has been completely transformed by the Internet of Things (IoT), which has applications in smart cities, industrial control systems, and healthcare. The Routing Protocol for Low-Power and Lossy Networks (RPL), a pillar of Internet of Things communications, is at the center of this technological revolution (Mayzaud et al., 2017). But as IoT deployments increase in quantity, so do the security issues they encounter; version number attacks, in particular, are becoming a serious danger to RPL-based networks. Specifically created for Internet of Things devices with limited resources, RPL arranges networks into Destination-Oriented Directed Acyclic Graphs (DODAGs). In low-power and lossy networks, this hierarchical structure facilitates effective routing, but it also

creates weaknesses that malevolent actors can take advantage of (Alsukayti & Singh, 2022). Attacks based on version numbers target RPL's global repair mechanism, which is a manipulable feature meant to preserve network topology. Version number attacks operate on a very straightforward but highly disruptive basis. An attacker can force an unneeded network rebuild by artificially increasing the DODAG version number. This can result in higher overhead, faster battery drain, and possibly even routing loops (Almusaylim et al., 2020). The consequences of such attacks go far beyond simple technological disruptions, as IoT networks increasingly support essential infrastructure, potentially jeopardizing both public safety and economic stability. Numerous mitigation solutions have been proposed recently, ranging from machine learning-based detection models (Osman et al., 2021) to distributed monitoring systems (Mayzaud et al., 2017). Nevertheless, these methods frequently fail to strike a compromise between strong security and IoT devices' energy limitations. Furthermore, there are still a lot of gaps in our knowledge of their actual effectiveness due to the dearth of thorough comparative research and sparse real-world testing in expansive settings (Nandhini et al., 2021). By creating an energy-aware, adaptive security framework especially designed to counter version number assaults in RPL-based IoT networks, our research seeks to close these gaps. We expand on previous work, fixing shortcomings and introducing novel ideas to produce a more all-encompassing solution. We will conduct a full review of current mitigation approaches, evaluating their strengths and limitations, in the parts that follow in this proposal. Describe the evolution of our adaptive detection system, which can dynamically adapt to changing attack patterns and network conditions. Explain our energy-efficient mitigation approach, which tries to fend off threats while using the fewest resources possible. Describe how to build an integrated security framework that combines fast recovery, mitigation, and detection techniques. Describe our approach to practical evaluation in several real-world IoT deployments, guaranteeing the solution's applicability in various contexts. Our research seeks not only to improve the security and reliability of present IoT installations but also to impact the future of IoT protocols and standards by tackling the fundamental vulnerability of version number attacks. Explore this all-encompassing approach to IoT security with us—it blends innovative theory with real-world application, and it could completely transform the way we safeguard our increasingly interconnected world. This study offers findings that could have a big impact on business practices and scholarly understanding of IoT security since it sits at the nexus of network security, IoT technology, and protocol design. As we explore

every facet of our suggested framework, we hope to keep readers interested by emphasizing the framework's potential for practical application and the innovative character of our method for resolving this pressing security issue.

Problem statement:

A serious security risk to Internet of Things (IoT) networks, especially in industrial control, smart cities, and healthcare systems, is version number assaults in Routing Protocol for Low-Power and Lossy Networks (RPL). The attacks target the global repair mechanism of RPL, resulting in the needless reconstruction of the Destination-Oriented Directed Acyclic Graph (DODAG). This process raises the overhead of the network, accelerates the depletion of batteries, and may create routing loops in Internet of Things devices. Developing an energy-aware, adaptive security framework to effectively combat version number assaults in RPL-based IoT networks while taking into account the resource limits of IoT devices is the main research question. The issue at hand is noteworthy because of the swift expansion and growing significance of Internet of Things implementations in vital infrastructure. Attacks using version numbers can significantly reduce the lifespan of networks, cause operational disruptions, and jeopardize data integrity. IoT-dependent industries run the risk of financial losses, privacy violations, and public safety issues as IoT networks grow more essential to critical systems. There are several notable gaps in the state of this field's study. First off, it is challenging to determine the relative efficacy of the various mitigation strategies now in use because to the conspicuous lack of thorough comparative research evaluating them. Second, an important overlook in present research efforts is that there are not many solutions that adequately balance strong security measures with the strict energy limits of IoT devices. Finally, there is a lack of real-world testing in large-scale IoT contexts for many of the suggested solutions, which raises concerns about their applicability and scalability in real deployment scenarios. It is imperative that this research question be addressed in order to guarantee the IoT networks' continuous growth, dependability, and public confidence. By creating and testing a novel, energy-efficient security framework that can adjust to different IoT device constraints and integrate with more comprehensive security measures, this study seeks to close these gaps and improve the overall security posture of RPL-based IoT networks against version number attacks.

Research objective:

Enhanced Investigation Goal: Developing, implementing, and evaluating a comprehensive, energy-efficient, and flexible solution for version number attack detection and mitigation in RPL-based IoT networks would help to increase the security and resilience of large-scale IoT installations.

To design and assess a security framework that is energy-efficient, adaptable, and incorporates detection, mitigation, and fast recovery mechanisms to mitigate version number threats in RPL-based IoT networks. To carry out a thorough comparative study of the mitigation strategies that are currently in use and to use the suggested solution in various real-world IoT deployments (smart city, industrial IoT, healthcare) in order to evaluate user acceptability, performance, and dependability. To measure key performance indicators as the size of the network increases and conduct a scalability analysis of the suggested solution in large-scale IoT networks (10,000+ nodes) using simulation and real-world testing. Using the study's findings as a basis, develop and submit evidence-based recommendations to the appropriate standardizing bodies for strengthening the RPL standard's inherent defenses against version number attacks.

This study is essential to safeguarding the growing field of Internet of Things implementations. Our goal is to increase the security, efficiency, and reliability of IoT systems dramatically by tackling the critical vulnerability of version number attacks in RPL-based networks. We will close the gap between academic research and practical application with our all-encompassing strategy, which combines theoretical study with practical execution and evaluation. Our solution is viable for resource-constrained IoT devices in large-scale deployments since it focuses on energy efficiency and scalability. Furthermore, this research has the ability to influence the direction of IoT network protocols in the future and leave a lasting legacy in the area by potentially aiding standardization efforts. A thorough evaluation of the versions number attack solutions currently in use with one another. A cutting-edge, flexible, and energy-saving version number attack detection and mitigation system. Factual information about how well the suggested solution works and how it affects actual Internet of Things deployments. Metrics for scaling IoT network security on a big scale. Improvements that should be made to the RPL standard to protect it from version number attacks. Quick recovery for network restoration following an attack. Additions to the corpus of knowledge on IoT security through presentations at international conferences and publications in journals of significant influence.

Research scope:

The goal of this research is to mitigate version number attacks in RPL-based IoT networks by defining distinct boundaries in various domains. The Routing Protocol for Low-Power and Lossy Networks (RPL) is the main focus of network protocol study, with particular attention paid to the Destination-Oriented Directed Acyclic Graph (DODAG) structure. Only in terms of comparison will other routing protocols be taken into account. Other attack types (such as sinkhole and blackhole) are only taken into consideration in connection with version number attacks or as part of the larger security framework. The attack vector analysis focuses on version number assaults within RPL. The study covers a variety of resource-constrained IoT devices that are commonly used in deployments, such as single-board computers (like the Raspberry Pi, Arduino), ESP32, and Nordic nRF52 specialized IoT modules, and low-power microcontrollers (like the ARM Cortex-M series). Excluded are high-performance gadgets that don't fit the usual IoT restrictions. Different testing environments will use different network scales: networks with 100–1,000 nodes will be tested in real-world settings, networks with 100–10,000 nodes in simulations, and networks with up to 100,000 nodes in theoretical modeling and extrapolation. Three main IoT application areas are the subject of this research: industrial IoT (manufacturing and process control), smart city infrastructure, and healthcare IoT. There will be a limited amount of research done in other areas (such smart homes and agriculture) in order to test generalizability. An integrated security framework, an energy-efficient mitigation technique, and an adaptive detection system for version number attacks are some of the security methods that will be created. For complete protection, the RPL security systems that are now in place will be integrated. Extensive analysis of cryptographic protocols that are not directly related to mitigating version number attacks is not included. Performance measurements will be centered on the following: recovery time and network resilience; energy consumption and device lifespan; detection accuracy and false positive rates; and scalability of security solutions. Comprehensive evaluation of metrics (such data throughput optimization) unrelated to security or energy efficiency is not included. The real-world testing will be conducted in partner organizations' genuine IoT environments, with the implementation environments predominantly using the Cooja simulator for Contiki-NG OS for simulations. Other simulation tools will be used sparingly and only for scenario testing or validation. The project will last for 24 months, and only the last five years' worth of RPL and IoT security research

will be taken into account for historical data. Future forecasts will only cover immediate effects and suggestions for the next one to three years. The Internet Engineering Task Force (IETF) RPL standard will be the primary focus of standardization activities; comprehensive analyses of the standardization procedures for other IoT protocols or broad cybersecurity standards will not be included. Analyzing the privacy implications of the suggested security measures as well as the moral implications of data collecting and analysis in IoT networks are examples of ethical and privacy considerations. Excluded is a thorough examination of IoT ethics that go beyond security and privacy. The geographic scope mostly concentrates on deployments in industrial and urban settings in developed nations, giving little thought to generalizability testing in rural or developing world situations. The data analysis will comprise qualitative analysis restricted to user acceptance and useful implementation feedback, as well as quantitative study of network performance and security parameters. The socioeconomic effects of enhanced IoT security are not thoroughly examined. Excluding full-scale commercial deployment concerns (TRL 8–9), the project seeks to attain Technology Readiness Level (TRL) 6-7 (technology demonstration in relevant environment) by its conclusion. This wide-ranging study scope balances analytical depth with real-world limitations and ethical considerations to provide a targeted but in-depth examination of version number attacks in RPL-based IoT networks.

Chapter 2

Literature review:

This paper proposes a distributed monitoring strategy to detect version number attacks in RPL-based Internet of Things networks. The authors develop algorithms for detecting attacks and identifying malicious nodes and implement their solution using a passive monitoring architecture with dedicated high-order nodes. They evaluate the performance through extensive simulations and quantify scalability using a monitoring node placement optimization method. Key findings show the strategy can effectively detect attacks with low false positive/negative rates and identify malicious nodes while having minimal impact on network operations. The primary drawbacks are as follows: 1) the method calls for the deployment of extra monitoring nodes, which raises the overall cost and complexity of the network; 2) the solution is tailored for RPL networks and might not translate to other IoT

routing protocols. The study does not state the precise dataset size utineeds to be in the simulations.(Mayzaud et al., 2017)

In order to prevent Version Number (VN) assaults in RPL-based IoT networks, this research study presents CDRPL (Collaborative and Distributed RPL), a lightweight security strategy. The goal was to provide a detection and mitigation system for VN attacks, both simple and composite, that is effective and doesn't add any complexity or costs. The process comprised altering RPL's capabilities to add a distributed and cooperative security mechanism. Although the study does not specify dataset sizes, it considered varying-scale network scenarios. The major conclusions demonstrate that CDRPL maintained network stability, controlled traffic overhead and QoS performance, and consumed energy in various VN attack situations while providing rapid and accurate attack detection and topology convergence. CDRPL produced better results with lightweight processing and reduced communication overhead as compared to similar techniques. The study was simulation-based rather than actual IoT devices, and the approach was only tested against VN attacks—not other kinds of RPL routing attacks—as the two key drawbacks seem.(Alsukayti & Singh, 2022)

The goal of this research article is to develop a Secure RPL Routing Protocol (SRPL-RP) for Internet of Things RPL networks that can identify, prevent, and isolate rank and version number assaults. The technique uses five phases: attack detection based on rank comparison, node authenticity checks, timestamp verification, mitigation utilizing attack status tables and thresholds, and isolation of rogue nodes. Simulation was used to assess the methodology; however, precise dataset size information was not given. The main conclusions indicate that SRPLRP improved with a 98.48% packet delivery ratio, a control message value of 991 packets/second, average energy usage of 1231.75 joules, and an accuracy rate of 98.17% against attacks. The primary restrictions seem to be: 1) Because the evaluation was simulation-based, there was no real-world implementation or testing on actual IoT devices. 2) There is a Lack of comparison with more RPL security systems now in use beyond the previously listed ones (Standard RPL with Attacks, SBIDS, and RPL+ Shield).((Almusaylim et al., 2020)

This study proposes a machine learning model called ML-LGBM—based on a Light Gradient Boosting Machine—to identify Version Number Attacks (VNAs) in RPL-based Internet of Things networks. The authors employed feature extraction and selection methods, improved LGBM parameters, and created a

sizable VNA dataset with 1,050,861 records. They achieved great performance (e.g., 99.6% accuracy) by evaluating the model using measures such as accuracy, precision, F-score, true negative rate, and false-positive rate. Compared to previous methods, the ML-LGBM model showed a quicker execution time (140.217 seconds) and reduced memory usage (347,530 bytes), which made it appropriate for IoT devices with limited resources. The primary restrictions seem to be: 1) Since the evaluation was conducted on simulated hardware rather than actual IoT gear, its results might not accurately represent real-world performance. 2) The model's deployment and integration into real-world IoT networks for real-time attack detection are not covered in the study (Osman et al., 2021)

This study suggests using the RPL routing protocol as a lightweight means of detecting and mitigating version number attacks (VNA) in Internet of Things networks. The technique uses parent supervision, where parent nodes keep an eye on their children's advertised version numbers and send DAO messages to the root node informing it of any suspicious increments. After that, the root adds this data to a network-wide blocklist of malicious nodes. Cooja simulations with a 16-node network topology conducted 20-minute runs to assess the solution. Key results indicate that, compared to an unprotected network under attack, the suggested method successfully reduces the effects of VNA on control overhead, energy consumption, packet delivery ratio, and latency. Additionally, the solution uses little RAM. There are two primary restrictions: 1) It's possible that the evaluation's tiny network size (16 nodes) does not accurately reflect more extensive IoT implementations. 2) Only one kind of attack (VNA) was considered, although actual IoT networks deal with several security risks at once. (Rouissat et al., n.d.)

This research article employs a Claim method to detect version number threats in RPL-based IoT networks. The aim of this study is to assess the impact of a proposed version of an attack detection mechanism on network performance. The paper uses the Cooja simulator to model assaults and build network topologies. Although the precise size of the dataset is not stated, 13% of the networks used in the simulations have malicious nodes. One of the most important discoveries is the application of a Claim method, which enhances attack detection by enabling nodes to confirm questionable version number changes by interacting with other nodes. Comparing the technique to networks under assault without the detection system, it is demonstrated to cut latency by 87% and enhance packet delivery ratio by 86%. There are two primary drawbacks to this approach: 1) It might be less successful if

several rogue nodes are operating simultaneously, and 2) The detection scheme's computational overhead and energy consumption for IoT devices with limited resources are not fully assessed.(Nandhini et al., 2021)

An Ensemble Learning based Network Intrusion Detection System (ELNIDS) is suggested in this research study to identify routing assaults in Internet of Things networks that are based on RPL. Four ensemble machine learning classifiers—Boosted Trees, Bagged Trees, Subspace Discriminant, and RUSBoosted Trees—are implemented and assessed by the authors. The models were trained and tested using the RPL-NIDDS17 dataset, which contained evidence of seven different kinds of routing assaults. According to the experimental results, RUSBoosted Trees had the best Area Under ROC curve (0.98), while the Boosted Trees ensemble achieved the maximum accuracy (94.5%). Packet sniffing, feature extraction, ensemble-based traffic analysis, and attack detection/notification are all supported by the proposed ELNIDS architecture. The following seem to be the main limitations: 1) No testing or implementation on IoT devices with limited resources to assess overhead and real-world performance. 2) Instead of using actual network traffic traces, a synthetic dataset is used. 3) Limited comparison with other cutting-edge RPL network intrusion detection techniques outside of the used ensemble approaches. Overall, the findings show that ensemble learning techniques have promise for IoT network intrusion detection; however, more testing in more practical deployment settings is required.(Sharma et al., 2023)

In this study, a Q-Learning based method for identifying version number assaults in RPL-based mobile IoT networks—QSec-RPL—is proposed. Based on DIO message counts, the method computes Q-values for nodes using Q-Learning, with a penalty for version number changes. Periodically, the sink node analyzes network behavior to do detection. Using Cooja and the Contiki operating system, simulation was used to assess the approach. Networks with up to 70 nodes and 50% mobile nodes were used. Key findings indicate that, particularly in mobile circumstances, the technique achieves an average accuracy of 91% in detecting attackers, with a considerable decline in packet delivery ratio under attack. Attacks also resulted in significant increases in power consumption and end-to-end latency, especially when the attackers were closer to the sink. The primary restrictions seem to be as follows: 1) Since the evaluation was simulation-based, there was no testing or implementation on actual IoT devices. 2) Scalability was only shown for 70 nodes. 3) Limited comparison with other cutting-edge RPL security strategies outside of conventional message authentication code methods. Overall, the findings show that Q-Learning has promise for lightweight intrusion detection in mobile IoT contexts;

however, more testing in more extensive and practical installations is required.(Sharma et al., 2023)

In order to enhance intrusion detection systems (IDS), this study suggests using a modified binary grey wolf optimization (MBGWO) approach for feature selection. By utilizing a multi-objective fitness function and including the omega wolf in the position update procedure, the method improves on the original binary grey wolf optimization (bGWO). The NSL-KDD dataset was used to assess the methods through support vector machine (SVM) classification. Key findings indicate that MBGWO selected only 14 characteristics and achieved 99.22% accuracy, 99.10% detection rate, and 0.0064% false positive rate. MBGWO showed a superior balance between optimizing accuracy and decreasing the amount of features when compared to other approaches. The primary restrictions seem to be: 1) Only the NSL-KDD dataset was used for evaluation, which means it might not accurately reflect network activity in the present day. 2) Neither real-time network data nor IDS setups were used to test the methodology. 3) A detailed analysis of the algorithm's computational complexity was lacking. Overall, the findings point to MBGWO's potential for effective feature selection in IDS; however, more testing on a variety of datasets and practical applications is required to completely confirm its efficacy.(Alzubi et al., 2020)

An strategy based on deep learning is presented in this research paper to identify routing threats in Internet of Things (IoT) networks. The process entails using the Cooja IoT simulator to generate high-fidelity attack data for networks with between 10 and 1000 nodes. Relevant features are then extracted, and deep neural network models are trained to detect attacks such as version number modification, lowered rank, and hello-flood attacks. The models obtain 99% F1-scores and up to 99.5% training accuracy, according to key results. A sizable IoT Routing Attack Dataset (IRAD) with up to 64 million data points was also generated by the investigation. The three key contributions are as follows: 1) creation of a comprehensive IoT attack dataset; 2) scalable deep learning methodology for IoT routing attack detection; and 3) highly accurate detection models for three types of routing assaults. Three forms of routing assaults were taken into consideration, and the computational complexity of the approach was not fully explored. These are some of the limitations of the evaluation, which was based on simulation rather than actual IoT devices. Overall, the findings show that deep learning has promise for Internet of Things security; however, more testing on various real-world IoT

deployments is required to completely confirm the method's efficacy.(yavuz et al., 2018)

Chapter 3

Methodology:

This all-inclusive solution employs a multifaceted, systematic strategy to mitigate version number threats in RPL-based IoT networks. The control and experimental groups are included in the study design in order to thoroughly assess the suggested solutions. The control group consists of a standard RPL-based Internet of Things network with 1000 nodes at first, but it can be scaled up to 10,000+ for extensive testing. It does not have any extra security features. We create four experimental groups: Group B uses our proposed adaptive detection mechanism; Group C uses our energy-efficient mitigation strategy; Group D uses our full integrated security framework. Group A uses the current mitigation techniques (e.g., VeRA, TRAIL, SVELTE). Each experimental group's size and scalability are identical to those of the control group. The technique includes ethical considerations as a critical component. All collected data is anonymized and securely encrypted to preserve data privacy; no personally identifiable information is obtained from IoT devices or network traffic. Organizations taking part in real-world testing are asked to provide written informed consent, outlining the study's goals, data gathering procedures, and possible dangers. Implementing measures to prevent the disruption of essential services during real-world testing and setting up procedures for the prompt termination of experiments in the event of unforeseen dangers are examples of risk mitigation strategies. An institutional ethics committee reviews the study protocol, which complies with all applicable national and international standards for network security and IoT research. Real-world testbeds and simulation environments both make samples easier to access. Large-scale virtual testbeds for RPL-based IoT networks are constructed using the Cooja simulator, which also implements intricate simulations of diverse IoT devices with varying resource limitations. Working with industry partners, real-world testbeds are created to access IoT installations in three different environments: industrial IoT, smart city infrastructure, and healthcare IoT. To guarantee representativeness, every real-world testbed consists of a variety of at least 100 physical devices. The term "device selection" refers to the wide variety of Internet of Things devices that differ in terms of memory, processing power, and energy efficiency. Both

hardware and software components are part of the infrastructure configuration. Hardware deployment combines more potent edge devices with resource-constrained IoT devices (like Arduino, Raspberry Pi, and ESP32) and software-defined radios for adaptable network design and attack simulation. RPL is implemented software-wise using the Contiki-NG operating system for Internet of Things devices, with specially designed modules for attack simulation, detection, and mitigation techniques. IoT devices are equipped with lightweight recording methods and strategically positioned network sniffers to capture security incidents, computational load, and energy usage. For initial testing and calibration, the testing environment consists of a controlled laboratory setting; for field testing, access to real-world IoT deployments is arranged through partnerships. Comparative, qualitative, and quantitative methods are all included in data analysis. Metrics including detection accuracy, false positive rate, energy consumption, influence on battery life, network overhead, latency, recovery time following attack mitigation, and scalability performance are the main focus of quantitative study. Regression analysis, inferential statistics (such as ANOVA and t-tests), and descriptive statistics are among the statistical techniques used. Semi-structured interviews with system administrators of actual deployments and theme analysis of comments are used in qualitative analysis to find trends in user acceptability and perceived efficacy. By employing established measurements and scenarios, comparative analysis compares the suggested solutions to mitigation strategies that are currently in use. The study is conducted in six discrete phases over a 24-month period. Phase 1 (3 months) includes a thorough examination of the available options and a review of the literature. Phase 2, which lasts for four months, is devoted to creating the adaptive detecting system. Phase 3 consists of four months devoted to developing the mitigation strategy for energy efficiency. Phase 4 (3 months): This phase builds the framework for integrated security. Phase 5 involves extensive simulations and real-world testing over a six-month period. Phase 6, which lasts for four months, includes thorough data analysis, framework optimization, the creation of suggestions for standardization, and the writing of research papers and reports.

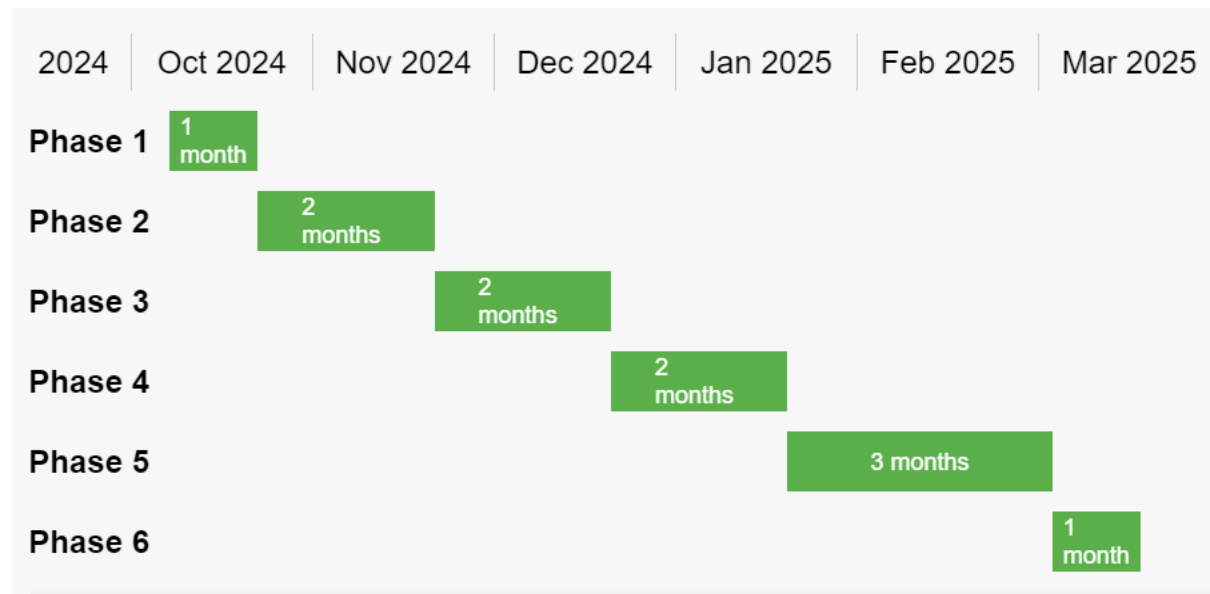
The methodology offers strategies for mitigating potential restrictions. Advanced simulation approaches and extrapolation methods are used to address scalability issues in testing very large networks. In order to manage device heterogeneity, different device selection in testbeds and the development of adaptive mechanisms are required. Adaptive algorithms and robustness testing with simulated network disruptions are used to accommodate for dynamic network conditions. Regular penetration testing and the use of a modular, easily updatable framework help to

meet the challenge of shifting attack techniques. This methodologically rigorous approach seeks to fully address the research objectives while upholding ethical norms and minimizing possible drawbacks. In order to ensure that the final integrated security architecture is strong, energy-efficient, and effective against version number assaults in RPL-based IoT networks, a multi-phase strategy to development and testing is used.

Expected outcomes:

By creating an energy-aware, adaptive security framework, this research seeks to solve the critical vulnerability of version number attacks in RPL-based IoT networks. The goals of the study are to develop an energy-efficient mitigation strategy, build an integrated security framework, analyze current mitigation techniques, and develop an adaptive detection system. Anticipated results include a thorough comparison of existing solutions, a novel detection system that is aware of context, an energy-efficient mitigation strategy, and an integrated security framework. The research will produce scalability analysis results for large-scale networks, real-world implementation results from various IoT contexts, and standardization proposals for improving RPL defenses. A quick recovery method, academic papers, improved simulation models, and technology transfer materials will also be produced by the project. By using this multimodal method, which combines theoretical innovation with practical implementation and real-world validation, the study aims to greatly increase IoT network security. It is anticipated that the resulting framework and techniques would have a significant impact on business practices and academic understanding of IoT security, especially in important areas like smart cities, industrial control, and healthcare systems.

Gantt chart :



References:

- Almusaylim, Z. A., Alhumam, A., Mansoor, W., Chatterjee, P., & Jhanjhi, N. Z. (2020). *Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things*. <https://doi.org/10.20944/preprints202007.0476.v1>
- Alsukayti, I. S., & Singh, A. (2022). A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks. *IEEE Access*, 10, 111115–111133. <https://doi.org/10.1109/ACCESS.2022.3215460>
- Alzubi, Q. M., Anbar, M., Alqattan, Z. N. M., Al-Betar, M. A., & Abdullah, R. (2020). Intrusion detection system based on a modified binary grey wolf optimisation. *Neural Computing and Applications*, 32(10), 6125–6137. <https://doi.org/10.1007/s00521-019-04103-1>
- Mayzaud, A., Badonnel, R., & Chrisment, I. (2017). A distributed monitoring strategy for detecting version number attacks in RPL-based networks. *IEEE Transactions on Network and Service Management*, 14(2), 472–486. <https://doi.org/10.1109/TNSM.2017.2705290>
- Nandhini, P. S., Srinath, P., Veeramanikandan, P., & Malliga, S. (2021). Version Attack Detection using Claim Algorithm in RPL based IoT Networks: Effects and Performance Parameters Evaluation. *Proceedings - 2nd International Conference on Smart Electronics and Communication, ICOSEC 2021*, 209–215. <https://doi.org/10.1109/ICOSEC51865.2021.9591735>

- Osman, M., He, J., Mokbal, F. M. M., Zhu, N., & Qureshi, S. (2021). ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks. *IEEE Access*, 9, 83654–83665. <https://doi.org/10.1109/ACCESS.2021.3087175>
- Rouissat, M., Universitaire Nour Bachir El Bayadh Mohammed BELKHEIR, C., Universitaire Nour Bachir El Bayadh Allel Mokaddem, C., Center Nour Bachir, U., Bachir, N., & Allel Mokaddem, A. (n.d.). *Parent supervision lightweight solution against version number attacks for IoT networks*. <https://doi.org/>
- Sharma, G., Grover, J., & Verma, A. (2023). QSec-RPL: Detection of version number attacks in RPL based mobile IoT using Q-Learning. *Ad Hoc Networks*, 142. <https://doi.org/10.1016/j.adhoc.2023.103118>
- yavuz, furkan, Yusuf YAVUZ, F., Ünal, D., & Gül, E. (2018). *Deep Learning for Detection of Routing Attacks in the Internet of Things*.