

Course Title: Research Methodology in Computer Science

Course Code: AI800

Weighting: 20%

Lecturer: Dr. Mohammed Anbar

Hand-out Date: 29 Jun 2024

Hand-in Date: 20 July 2024

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

Assignment Report: literature Review Detection System for RPL security



Table of contents:

- Summary research paper's
- Critical Analysis:
- Connections
- Conflicts between the findings
- Synthesis Matrix for Literature Review:
- References

Summary research paper's:

Paper1: A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks

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 bein the simulations.(Mayzaud et al., 2017)

Paper2: A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks

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)

Paper3: Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things

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 SRPL-RP 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)

Paper4: ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks RPL-Based Networks

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)

Paper5: Parent supervision lightweight solution against version number attacks for IoT networks

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.)

Paper6: Version Attack Detection using Claim Algorithm in RPL based IoT Networks: Effects and Performance Parameters Evaluation

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)

Critical Analysis:

Strengths and shortcomings are included in the research on version number attack detection in RPL-based IoT networks. The papers take a complete approach to addressing a pertinent security issue, through performance evaluations through extensive experiments, dedicated algorithms, and distributed monitoring systems. Research on Advanced Measurement Infrastructures (AMI) is more practically relevant when scalability and practical applicability are considered. However, some significant flaws include the monitoring strategy's possible overhead, the restricted scope that mainly concentrates on version number attacks, and the dependence on very inventive devices. There is little discussion of incorrect information and no comparison analysis with current methods

Both the good and the negatives can be improved. From a methodological standpoint, using simulation to assess performance makes sense; nevertheless, reproducibility might benefit from additional information about certain datasets or parameters. Although the research contributes significantly to RPL security in IoT networks, there is room to grow, overcome obstacles, and offer more thorough comparisons with current methods. The practical applicability of the suggested methods would be improved by more investigation into the trade-offs between resource utilization and security enhancements.

Connections:

- 1- **Focus on RPL protocol:** The RPL (Routing Protocol for Low-Power and Lossy Networks) protocol, frequently used in Internet of Things networks, is the subject of all the articles' security-related concerns.
- 2- Version number assaults: Several articles have discussed version number attacks on RPL networks, demonstrating that they are a serious security risk.
- 3- **Detection and mitigation:** A unifying objective among researchers is seen in the papers' general intent to identify and mitigate version number attacks.
- 4- Performance evaluation: The majority of research contains experimental analysis or performance evaluation in one form or another to validate suggested solutions.
- 5- **Lightweight solutions:** Considering the resource limitations of Internet of Things devices, several studies highlight the necessity for lightweight solutions.

Conflicts between the findings:

- 1- **Distributed vs. centralized:** While some studies support distributed methods, others suggest centralized monitoring options. For instance, a distributed monitoring architecture is expressly promoted in the publication "A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks."
- 2- **Monitoring techniques :** appear to be divided into two categories: active monitoring methods, which include target node cooperation, and passive monitoring techniques. The distributed monitoring study discusses this distinction in detail.
- 3- **Rule-based vs. machine learning:** While some articles (e.g., "ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks") seem to rely more on rule-based detection techniques, others may use machine learning techniques.

- 4- Attack mitigation scope:** While some articles (such as "Detection and Mitigation of RPL Rank and Version Number Attacks") concentrate exclusively on version number attacks, others (such as this one) handle several RPL attack types at once.
- 5- Parent supervision vs. network-wide monitoring:** In contrast to other articles offering more comprehensive network monitoring tactics, the study "Parent supervision lightweight solution against version number attacks for IoT networks" suggests a more focused approach focusing on parent nodes.

Synthesis Matrix for Literature Review:

Study	Authors	Year	Research Design	Key Findings/Results	Methodology	Limitations
A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks	Mayzaud et al.	2017	Experimental	The suggested distributed monitoring approach detected version number attacks with a detection rate of above 90%. In most cases, the false positive rate is less than 10%. The monitoring solution's communication overhead is between 15% and 20%. Energy usage rose by 5–10% as compared to networks that were not monitored. When maximizing monitor location, the solution expands effectively to	Data collection: RPL network simulation with Contiki OS's Cooja simulator The amount of the dataset was not stated clearly, yet several simulations were run. Number of samples: Tested networks with 20–100 nodes Preprocessing the dataset: N/A (using simulated data) Model development: Created methods for	assessed solely in virtual settings; actual IoT hardware is not used concentrated only on version number attacks and ignored other RPL flaws assumed that a few nodes with more capacity were available for monitoring tasks did not take into account extremely

				larger networks with more than 100 nodes.	distributed monitoring to identify version number attacks Training and testing of models: developed and put into use algorithms in virtual networks Assessment: Calculated false positive rate, communication overhead, and detection rate Performance measures include energy consumption, communication overhead, false positives, and detection accuracy.	dynamic topologies or node mobility limited assessment of the effect on regular network operations
A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks	IBRAHIM S. ALSUKAYTI AND AMAN SINGH	2022	Experimental	CDRPL offered precise and quick assault detection. It made topology convergence faster in the event of an attack. Throughout several VN attack scenarios, the approach effectively preserved network stability, control traffic overhead, QoS performance, and energy usage. When compared to other comparable methods, CDRPL performed better since it required reduced communication overhead, no extra entities, and lightweight node-local processing.	For RPL-based IoT networks, the researchers created a novel security plan known as CDRPL (Collaborative and Distributed scheme for RPL) to counteract Version Number (VN) threats. They made minor adjustments to the RPL protocol's capabilities in order to incorporate CDRPL. Tests were carried out to assess CDRPL, most likely with the aid of network simulation tools	For RPL-based IoT networks, the researchers created a novel security plan known as CDRPL (Collaborative and Distributed scheme for RPL) to counteract Version Number (VN) threats. They made minor adjustments to the RPL protocol's capabilities in order to incorporate CDRPL. Tests were carried out to assess CDRPL, most

					(although the snippet provided does not specify which tools were used). CDRPL was tested in various network scale scenarios against basic and composite VN attacks using different experimental configurations. Based on the previously indicated results, performance measures that were likely assessed were attack detection accuracy, topology convergence time, network stability, control traffic overhead, QoS performance, and energy consumption.	likely with the aid of network simulation tools (although the snippet provided does not specify which tools were used). CDRPL was tested in various network scale scenarios against basic and composite VN attacks using different experimental configurations. Based on the previously indicated results, performance measures that were likely assessed were attack detection accuracy, topology convergence time, network stability, control traffic overhead, QoS performance, and energy consumption.
Detection and Mitigation of RPL Rank and Version Number Attacks in Smart Internet of Things	Zahrah A. Almusaylim1 , Abdulaziz Alhumam2 , Wathiq Mansoor3 , Pushpita Chatterjee4 , NZ Jhanjhi5	2020	Experimental	High packet delivery rate (98.48%), low control message overhead (991 packets/second), and low energy usage (1231.75 joules) are all achieved by the SRPL-RP in the face of attacks. It has a high detection and mitigation accuracy rate of 98.17% for rank and version number attacks.	A comparison of ranks strategy serves as the basis for the detection. Attacks status tables and thresholds are used in the mitigation. The isolation notifies pertinent nodes to avoid identified attackers by adding them to a	There is no testing or real-world implementation; the evaluation is restricted to simulation-based analysis. The computational overhead and processing complexity

					blacklist table. The protocol is extensively tested against other RPL protocols in attack scenarios and supports a wide range of network topologies.	brought about by the suggested SRPL-RP protocol are not examined in this research.
ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks	MUSA OSMAN , JINGSHA HE , FAWAZ MAHIUOB MOHAMMED MOKBAL ,NAFEI ZHU , AND SIRAJUDDIN QURESHI	2021	Experimental	99.6% F-score, 99% precision, and 99.6% accuracy were attained. 99.3% of true negatives and 0.0093 of false positives 140.217 seconds were needed for execution. utilization of 347,530 bytes of memory outperformed alternative ML algorithms in terms of resource efficiency and accuracy.	Data gathering: Utilized Contiki OS and the Cooja simulator to produce network traffic data IoT networks based on RPL simulations, with 1-3 attacker nodes executing Version Number Attacks and 10–20 client nodes gathered unprocessed network traffic data with the 6LoWPAN analysis tool 1,050,861 instances in a	Perhaps the simulated environment doesn't accurately depict real-world IoT networks. restricted to merely detecting Version Number Attacks Large-scale IoT installations might not be feasible with small-scale simulation (10–20 nodes). Possible imbalanced dataset overfitting (more benign than harmful samples) Cross-validation,

					generated dataset (884,861 benign, 166,000 malicious) Preprocessing of the dataset: taken 113 characteristics out of the raw data. 59 features remaining after duplicates were eliminated. After deleting fixed and hexadecimal features, the features were further reduced to 17. Categorical features encoded Features normalized with min-max scaling Model creation: used Sequential Forward Selection for feature selection using the Light Gradient Boosting Machine (LightGBM) algorithm Enhanced LightGBM settings Training and testing of models: Divide data into sets for testing and training (exact split not specified). LightGBM model was trained using training data. Model performance tested on test data	which measures the generalizability of a model, is not mentioned. Not specifically tested performance in IoT devices with limited resources
--	--	--	--	--	---	--

					Assessment: criteria such as F-score, accuracy, precision, true negative rate, and false positive rate were employed. in comparison to other ML algorithms in terms of performance and resource use	
Parent supervision lightweight solution against version number attacks for IoT networks	Mehdi Rouissat Mohammed BELKHEIR Allel Mokaddem	2023	Experimental	In the simulated Internet of Things network, the suggested lightweight approach was able to identify and counter version number threats. instead of creating new message types, made use of the RPL control messages already in place. didn't need specific monitoring nodes or encryption Capable of retrieving every victim node, even those that are isolated Using the root node, decentralized detection is combined with centralized control.	Data collection methods: Simulations were conducted using Cooja, a Java-based network simulator Network topology of 16 nodes was used, with 1 malicious node placed 2 hops away from the root Z1 motes were simulated, based on MSP430 microcontrollers with CC2420 radio transceivers Each simulation ran for 20 minutes	tested solely with a modest 16-node topology restricted to simulation as opposed to actual deployment evaluated solely in relation to one kind of attack (version number assault) Performance comparison not made with other defense strategies, only with the baseline no-attack scenario The maximum

					Dataset/Sample size: 16 node network topology (15 legitimate nodes, 1 malicious node) Dataset preprocessing: Not explicitly mentioned, likely minimal as this was a simulation study Model development: Proposed a lightweight detection algorithm based on parent nodes supervising version numbers advertised by child nodes Uses existing RPL control messages (DIO, DAO) with added flags/tags to communicate suspicious behavior No machine learning models were developed Model training and testing: Algorithm was implemented and tested in the Cooja simulator Compared performance against baseline scenario with no attack Evaluation metrics: Control packet overhead (DIO and DAO)	simulation run duration is twenty minutes. ignored node mobility in favor of a static network design.
--	--	--	--	--	--	---

					messages) Energy consumption (LPM, CPU, TX and RX) Packet Delivery Ratio (PDR) Latency Memory footprint (RAM and ROM usage) Model creation: suggested a simple detection method based on parent nodes monitoring the version numbers that child nodes advertise. use already-existing RPL control messages (DAO, DIO) to communicate suspicious activity by adding flags or tags. There were no machine learning models created. Training and testing of models: The Cooja simulator was used to implement and test the algorithm. Performance was compared against an attack-free baseline scenario. Evaluation metrics: Overhead in control packets (DIO and DAO messages) Energy usage (CPU, TX,	
--	--	--	--	--	---	--

					RX, and LPM) PDR, or packet delivery ratio Lateness Memory footprint (use of RAM and ROM)	
Version Attack Detection using Claim Algorithm in RPL based IoT Networks: Effects and Performance Parameters Evaluation	P.S.Nandhini P.Srinath P.Veeramanikandan S.Malliga	2021	Experimental	Version attacks in RPL cause DODAG formations frequently, which in turn generate a lot of control packets and deteriorate network performance. In RPL-based IoT networks, the suggested Claim algorithm can successfully identify version attacks.	Methods: The RPL protocol's operation throughout the establishment and upkeep of the DODAG (Destination-Oriented Directed Acyclic Graph) topology is covered in this study. It outlines the current defenses against	The proposed Claim algorithm's performance evaluation and comprehensive experimental results are absent from the study. The quantity and makeup of the data

					version attacks in RPL and suggests a Claim mechanism for doing so. Data Set Size: The size of the data set utilized for the experiments is not mentioned in detail in the study.	collection used for the trials are not disclosed in the study.
--	--	--	--	--	---	---

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>
- 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/>