

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

Student Name: Mohammed Yahya Alghazwani

Student ID: 261002006

Section: artificial intelligence

Table of contents:

1- Summary research paper's

2- Critical Analysis

3-Connections

4-Conflicts between the findings

5-Synthesis Matrix for Literature Review

6- References

Summary research paper's

Paper 1 – 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 introduce monitoring nodes that observe network behavior and identify malicious nodes that manipulate the version number in RPL messages. The solution is evaluated using simulation and shows that the proposed monitoring architecture can detect attacks effectively with low false positive and false negative rates. The study also analyzes scalability and the placement of monitoring nodes to improve detection efficiency. However, the method relies mainly on simulation and may require additional evaluation in real IoT environments.

Paper 2 – Intrusion Detection System Based on a Modified Binary Grey Wolf Optimisation

This research presents an intrusion detection system that uses a modified binary grey wolf optimization algorithm for detecting network attacks. The proposed model improves feature selection by using optimization techniques inspired by grey wolf hunting behavior. The method aims to enhance detection accuracy and reduce computational complexity in intrusion detection systems. Experimental results show improved detection performance compared to traditional approaches. The main limitation is that the algorithm requires careful parameter tuning and may increase computational cost when applied to large datasets.

Paper 3 – Parent Supervision Lightweight Solution Against Version Number Attacks for IoT Networks

This study proposes a lightweight mechanism to detect and mitigate version number attacks in IoT networks using the RPL protocol. The technique is based on parent supervision, where parent nodes monitor the version numbers announced by their child nodes. If abnormal increments are detected, the information is sent to the root node, which maintains a blacklist of malicious nodes. Simulation results show that the proposed method reduces control overhead and energy consumption while improving network stability. However, the approach may depend heavily on the reliability of parent nodes and may face challenges in large-scale networks.

Paper 4 – ELNIDS: Ensemble Learning Based Network Intrusion Detection System for RPL Based Internet of Things

This paper proposes an ensemble learning-based intrusion detection system for RPL-based IoT networks. The authors combine multiple machine learning algorithms to improve attack detection accuracy. The system analyzes network traffic features and classifies them using ensemble learning techniques. Experimental results show that the model achieves high detection accuracy and improves the overall performance of intrusion detection systems. The study demonstrates that combining multiple classifiers enhances reliability and reduces false detection rates. However, ensemble models may increase computational overhead compared to single classifier approaches.

Paper 5 – Version Attack Detection Using Claim Algorithm in RPL Based IoT Networks

This paper introduces a claim-based algorithm for detecting version number attacks in RPL-based IoT networks. The proposed method verifies the version numbers broadcast by nodes and compares them with claims received from neighboring nodes. If inconsistencies are detected, the system identifies malicious nodes and prevents them from affecting the network topology. Simulation results show improvements in packet delivery ratio, network stability, and energy efficiency. The limitation of this work is that the evaluation is mainly simulation-based and may require further real-world validation.

Paper 6 – ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks

This research proposes a machine learning-based detection model called ML-LGBM for identifying version number attacks in RPL-based IoT networks. The approach uses the Light Gradient Boosting Machine algorithm along with feature extraction and feature selection techniques. A large dataset was generated using network simulations to train and evaluate the model. Experimental results show that the proposed method achieves very high accuracy in detecting attacks while maintaining low computational overhead. The study concludes that ML-LGBM is suitable for resource-constrained IoT devices, although the dataset includes only one type of attack.

Critical Analysis – Connections

All selected studies focus on improving the security of IoT networks that use the RPL routing protocol. Most of the papers address version number attacks, which are among the most critical attacks affecting network stability and resource consumption. Several approaches are proposed including monitoring systems, parent supervision techniques, claim-based algorithms, and machine learning models. The studies also rely heavily on simulation environments such as Cooja to evaluate their solutions. Overall, the research demonstrates a growing trend toward integrating intelligent detection mechanisms, especially machine learning, to improve intrusion detection performance in IoT environments.

Conflicts Between the Findings

Although the studies share the same objective of detecting RPL attacks, they differ in the techniques used and the results obtained. Some studies rely on lightweight rule-based mechanisms which focus on minimizing computational overhead. In contrast, other studies use machine learning and ensemble learning techniques, which achieve higher detection accuracy but may require more computational resources. Additionally, some research emphasizes energy efficiency and network overhead reduction, while others focus mainly on improving detection accuracy and classification performance.

Synthesis Matrix for Literature Review

Paper	Method	Dataset / Simulation	Main Contribution	Limitation
Distributed Monitoring Strategy	Distributed monitoring	Simulation	Detects malicious nodes with low error rate	Needs real environment testing
Grey Wolf IDS	Optimization algorithm	Dataset analysis	Improves feature selection and detection accuracy	High computational cost
Parent Supervision	Lightweight monitoring	Cooja simulation	Reduces energy consumption and overhead	Depends on parent node reliability
ELNIDS	Ensemble learning	Network traffic dataset	High detection accuracy	Higher computational complexity
Claim Algorithm	Verification mechanism	Simulation	Improves network stability	Limited real-world validation
ML-LGBM	Machine learning	Large simulated dataset	Very high detection accuracy	Only one attack type tested

References

A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks. [RPL security – Dropbox](#)

Intrusion Detection System Based on a Modified Binary Grey Wolf Optimisation. [RPL security – Dropbox](#)

Parent Supervision Lightweight Solution Against Version Number Attacks for IoT Networks. [RPL security – Dropbox](#)

ELNIDS: Ensemble Learning Based Network Intrusion Detection System for RPL Based Internet of Things. [RPL security – Dropbox](#)

Version Attack Detection Using Claim Algorithm in RPL Based IoT Networks. [RPL security – Dropbox](#)

ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks. [RPL security – Dropbox](#)