

- **Course Title:** Research Methodology in Computer Science
- **Course Code:** AI800
- **Lecturer:** Dr. Mohammed Anbar
- **Student Name:** Abdulrahman Ali Ghibban
- **Student ID:** 261001713
- **Hand-out Date:** 21 Feb 2026
- **Hand-in Date:** 7 Mar 2026
- **Hand-in Method:** Online Submission via E-Learning.

Assignment report : Comprehensive Literature Review Advancements in AI-Driven and Algorithmic Security for RPL-Based IoT Networks

Table of contents:

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

2. Summary of Research Papers

Paper 1: Distributed Monitoring for Version Number Attacks (Mayzaud et al., 2017)

In this seminal work, Mayzaud et al. address the inherent vulnerability of the Routing Protocol for Low-Power and Lossy Networks (RPL) to version number (VN) attacks by proposing a distributed monitoring architecture. Unlike centralized approaches that may succumb to single-point-of-failure risks, this strategy utilizes dedicated high-order nodes to perform passive monitoring. The authors introduce sophisticated algorithms for identifying malicious actors while employing a placement optimization method to ensure scalability across varying network densities. Empirical data derived from Cooja simulations suggests a robust efficacy, with detection rates exceeding 90% and false positive rates remaining below 10%. However, from an evaluative standpoint, the necessity of deploying specialized monitoring entities introduces a tangible increase in network complexity and capital expenditure. Furthermore, while the 15–20% communication overhead is documented, the lack of a specified dataset size somewhat obscures the absolute statistical power of the results. It appears that while the framework is technically sound, its strict optimization for RPL environments may limit its utility in heterogeneous IoT ecosystems where multiple routing protocols coexist.

Paper 2: Collaborative and Distributed RPL (Alsukayti & Singh, 2022)

The Collaborative and Distributed RPL (CDRPL) scheme represents a significant pivot toward lightweight security by modifying existing protocol capabilities rather than introducing external hardware. The authors aim to mitigate both simple and composite version number attacks by embedding security logic directly into node-local processing. This approach appears particularly prudent given the extreme resource constraints of typical IoT devices. The research demonstrates that CDRPL effectively preserves network stability and Quality of Service (QoS) across varying scales, achieving rapid topology convergence without the energy tax associated with heavy cryptographic primitives. While the results suggest a superior performance regarding communication overhead, the methodological reliance on simulation-only environments represents a notable boundary. One might argue that the failure to test against a broader spectrum of RPL routing attacks, such as rank or blackhole assaults, limits the perceived resilience of the CDRPL framework. Nevertheless, the study provides a compelling case for "in-protocol" security enhancements as a viable alternative to dedicated monitoring infrastructures, provided that the increased processing load remains within acceptable limits.

Paper 3: The SRPL-RP Protocol (Almusaylim et al., 2020)

Almusaylim et al. propose the Secure RPL Routing Protocol (SRPL-RP), a multifaceted defense mechanism designed to identify and isolate both rank and version number assaults. The methodology is technically dense, structured around five rigorous phases: rank-based attack detection, node authenticity validation, timestamp verification, mitigation via attack status tables, and the final isolation of rogue nodes. This procedural depth likely accounts for the impressive **98.17% accuracy rate** and the **98.48% packet delivery ratio (PDR)** reported. Furthermore, the protocol demonstrates a managed control message overhead of 991 packets/second and an average energy footprint of 1231.75 joules. Despite these quantitative successes, a critical lens reveals a significant benchmarking gap; the authors primarily compare SRPL-RP against standard RPL and the RPL+ Shield, neglecting more contemporary AI-driven

models. Additionally, the lack of real-world implementation on physical IoT hardware leaves the protocol's performance in the face of stochastic signal interference largely theoretical. The use of timestamp verification and status tables, however, provides a promising blueprint for temporal-based security in lossy environments.

Paper 4: Machine Learning via LightGBM (Osman et al., 2021)

The ML-LGBM model introduces a sophisticated data-driven paradigm to IoT security, utilizing the Light Gradient Boosting Machine to detect version number attacks. The authors' methodology is remarkably rigorous, beginning with a massive dataset of 1,050,861 records (comprising 884,861 benign and 166,000 malicious samples). By employing Sequential Forward Selection, the researchers distilled 113 raw features down to 17 high-impact variables, optimizing the model for resource-constrained environments. This meticulous feature engineering resulted in a **99.6% accuracy** and a matching 99.6% F-score, alongside a 99.3% true negative rate. Technical efficiency is further evidenced by a 140.217-second execution time and a modest memory footprint of 347,530 bytes. However, an academic researcher must question the potential for overfitting given the imbalanced nature of the dataset and the lack of testing on physical IoT gear. While the model outperforms traditional machine learning algorithms in a virtualized context, the study fails to detail the practical integration of such a model into the live, real-time firmware of low-power motes, leaving a gap between algorithmic excellence and operational reality.

Paper 5: Parent Supervision Mechanism (Rouissat et al., 2023)

Rouissat et al. present a lightweight parent supervision mechanism that eschews dedicated monitoring nodes in favor of utilizing existing DAO and DIO messages. By tagging these control messages with flags, parent nodes can monitor the version number increments of their children and report suspicious behavior to the root node, which maintains a network-wide blocklist. The study's evaluation utilized Cooja simulations of Z1 motes (MSP430-based) over 20-minute runs. While the findings suggest the solution is capable of retrieving all victim nodes and reducing energy consumption compared to undefended networks, the methodology is constrained by its scale. The use of a 16-node topology with only a single malicious node situated two hops from the root may not adequately simulate the cascading failures found in dense smart city deployments. Furthermore, the absence of a performance comparison against other modern defense strategies—relying instead on a baseline "no-attack" scenario—limits the ability to gauge where this supervision mechanism sits within the current competitive landscape of IoT security.

Paper 6: The Claim Algorithm (Nandhini et al., 2021)

The "Claim algorithm" is introduced as a peer-based verification mechanism where nodes within a DODAG interact to confirm the legitimacy of version number changes. The researchers focus on the deleterious effects of frequent DODAG reformations, which typically degrade network performance through excessive control packet generation. By implementing the Claim algorithm, the study reports an 86% enhancement in PDR and a significant **87% reduction in latency**. In simulations where 13% of the network consisted of malicious nodes, the algorithm successfully identified version attacks that would otherwise cause total network instability. However, the academic validity of the work is slightly hampered by the omission of the precise dataset size and the failure to fully assess the computational overhead and energy costs associated with peer-to-peer verification. One might suspect that the collaborative nature of the "Claim" process could introduce a new vector for collusion if multiple rogue nodes coordinate their claims. Future research would need to address this potential for sybil-style or coordinated attacks to ensure the algorithm's long-term viability.

3. Critical Analysis

The collective research into RPL-based security reveals a clear evolution from heavy cryptographic dependencies toward lightweight, "protocol-aware" algorithmic solutions. This trajectory is logical; the resource-constrained nature of IoT devices—often running on limited battery power and minimal RAM—necessitates security measures that do not jeopardize the primary routing function. The high accuracy rates reported across the literature, often exceeding 98%, suggest that the theoretical detection of Version Number Attacks has reached a high level of maturity.

However, a profound "Simulation Gap" remains the most significant methodological obstacle in this field. As observed in the work of Rouissat et al. (2023) and Nandhini et al. (2021), there is a persistent reliance on the Cooja simulator. While Cooja is a vital tool for early-stage prototyping, it often provides a sanitized environment that fails to capture the stochastic nature of real-world IoT deployments. Virtualized environments typically abstract away the complexities of signal fading, physical electromagnetic interference, and the non-linear battery depletion cycles that characterize physical hardware. Consequently, the high PDR and low energy usage metrics achieved in a laboratory setting may not be reproducible when these protocols are ported to actual physical testbeds.

Furthermore, the methodological reliance on small-scale topologies is a concerning limitation that threatens the generalizability of these findings. The 16-node limit utilized by Rouissat et al. and the 10–20 node scenarios in Osman et al.'s machine learning research are insufficient to model the complexities of industrial IoT or smart city applications. In larger, more dynamic networks, the overhead of "Distributed Monitoring" (Mayzaud et al.) or the "Claim Algorithm" (Nandhini et al.) may scale non-linearly, potentially leading to congestion or total network collapse.

Finally, the lack of testing on physical Z1 motes or modern hardware variants is a missed opportunity. While many studies simulate the MSP430 architecture, they rarely account for the physical constraints of the CC2420 radio transceivers or the impact of environmental obstacles on packet delivery. To bridge this gap, future research must move beyond purely simulated "perfect" environments and embrace heterogeneous, physical hardware testing to validate that these AI-driven models are truly resilient in the field.

4. Connections: Shared Research Trajectories

- **RPL-Centric Security:** All six papers converge on the RPL protocol as the primary point of vulnerability in low-power networks, specifically identifying the Version Number (VN) attack as a uniquely destructive threat to DODAG stability and energy longevity.
- **The Push for Lightweight Design:** A distinct research trajectory links Alsukayti & Singh (2022) with Rouissat et al. (2023) regarding the absolute necessity of maintaining low RAM and energy footprints. Both studies prioritize the modification of existing protocol messages (DAO/DIO) over the introduction of resource-heavy cryptographic entities.
- **Performance Validation Standards:** There is a universal shared reliance on Packet Delivery Ratio (PDR), energy consumption (often measured in Joules or through CPU/TX/RX cycles), and control message overhead as the "gold-standard" metrics for validating the success of security mechanisms.

5. Conflicts and Theoretical Divergence

Distributed vs. Centralized Architectures

A fundamental philosophical divide exists between the distributed monitoring strategy of Mayzaud et al., which advocates for localized detection via high-order nodes, and the centralized control proposed by Rouissat et al. While Mayzaud's distributed approach offers superior scalability for large networks, it incurs higher deployment costs; conversely, Rouissat's parent-to-root centralized model simplifies management but risks creating a communication bottleneck at the root node.

Rule-based vs. Machine Learning Logic

Theoretical divergence is evident when comparing the algorithmic logic of the "Claim Algorithm" (Nandhini et al.) with the data-driven ML-LGBM model (Osman et al.). Rule-based algorithms offer deterministic and transparent detection but may lack the adaptive flexibility of Osman's machine learning approach, which identifies complex patterns across 1,050,861 data records using Sequential Forward Selection.

Passive vs. Active Monitoring

The trade-offs between monitoring methodologies remain contested. Mayzaud et al. advocate for dedicated, passive monitoring nodes to minimize disruption to legitimate traffic. In contrast, Almusaylim et al. utilize active protocol modifications (SRPL-RP) that integrate detection directly into the routing process, potentially increasing the processing load on every legitimate node within the network.

6. Synthesis Matrix for Literature Review

Study (Author/Year)	Research Design	Key Findings/Metrics	Methodology	Critical Limitations
Mayzaud et al. (2017)	Experimental	>90% detection; <10% false positive; 15-20% comm overhead; 5-10% energy increase.	Distributed monitoring; Cooja; placement optimization; 20-100 nodes.	Requires extra monitoring nodes; limited to RPL; no dataset size stated.
Alsukayti & Singh (2022)	Experimental	Rapid detection; maintained QoS/stability; low overhead; faster topology convergence.	CDRPL scheme; modified RPL capabilities; various scale scenarios.	Tested only against VN attacks; no testing on actual physical devices.
Almusaylim et al. (2020)	Experimental	98.48% PDR; 98.17% accuracy; 991 packets/sec overhead; 1231.75 J usage.	SRPL-RP; 5 phases (rank comparison, status tables, timestamp verification).	No real-world implementation; lack of comparison with modern AI security.
Osman et al. (2021)	Experimental	99.6% accuracy; 99.6% F-score; 140.217s	ML-LGBM; 1,050,861 records;	Simulated hardware only; 10-20 nodes too

		execution; 347,530 bytes RAM usage.	Sequential Forward Selection (113 to 17 features).	small for scale; possible overfitting.
Rouissat et al. (2023)	Experimental	Effective VNA reduction; low RAM usage; identifies isolated nodes via root blacklist.	Parent supervision; Cooja; 16-node topology; Z1 motes (MSP430); 20-min runs.	Small network size; single attack type; no comparison with other defense strategies.
Nandhini et al. (2021)	Experimental	87% latency reduction; 86% PDR enhancement; 13% malicious node density.	Claim algorithm; peer interaction within DODAG; Cooja simulator.	Ineffective against coordinated rogue nodes; computational overhead not fully assessed.

7. 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. *Preprints*. <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. *2021 5th International Conference on Computing Methodologies and Communication (ICCMC)*.
- Osman, M., He, J., Mohammed Mokbal, F. 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, 83631–83645. <https://doi.org/10.1109/ACCESS.2021.3086358>
- Rouissat, M., Belkheir, M., & Mokaddem, A. (2023). Parent supervision lightweight solution against version number attacks for IoT networks. *Journal of Reliable Intelligent Environments*.